Observatorio Centroamericano de Seguridad Digital

- Informe anual 2016 -

El Salvador

HlqVRomqgghOAC
j86Z/sIDhll vy5Wvr

Observatorio Centroamericano de Seguridad Digital

- Informe anual 2016 -

El Salvador

Observatorio Centroamericano de Seguridad Digital

Informe anual 2016

El Salvador[1]

INTRODUCCIÓN

El Observatorio Centroamericano de Seguridad Digital (OSD) surge como una iniciativa de Fundación Acceso que logra consolidarse en el año 2016.

El objetivo general del OSD es registrar y analizar incidentes de seguridad digital de personas defensoras de DDHH que estén ejerciendo su defensoría en El Salvador, Guatemala, Honduras y/o Nicaragua.

Para alcanzar este objetivo, Fundación Acceso visita y da seguimiento a las personas u organizaciones defensoras de DDHH que reportan un incidente a su seguridad digital, lleva un registro de los incidentes reportados y elabora un informe anual con la información recolectada.

Con esto se busca fortalecer los mecanismos de seguridad de defensores/as de DDHH, posicionar el tema de la seguridad digital como un componente clave de la seguridad integral, fortalecer el análisis de la seguridad integral de defensores/as de DDHH en Centroamérica y apoyar potenciales litigios estratégicos con información basada en análisis jurídico e informático.

a) ¿Qué es un incidente de seguridad digital?

El Observatorio Centroamericano de Seguridad Digital registrará aquellos incidentes ocurridos a personas defensoreas de DDHH en Centroamérica relacionados con su información y/o comunicación digital almacenada, en movimiento y en servicios.

Por defensor/a de derechos humanos tomamos el concepto amplio que se maneja en la declaración de Naciones Unidas[2], considerando individuos, grupos e instituciones de quienes tengamos referencia que luchen por la defensa de derechos humanos de los pueblos y las personas

1. El capítulo de El Salvador ha sido elaborado por el asesor legal en el país, Marlon Hernández Anzora, con el apoyo de los técnicos David Oliva y Arturo Chub, y de la Encargada de Desarrollo Organizativo, Luciana Peri.

2. Organización de Naciones Unidas, Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos. Disponible en http://www.ohchr.org/Documents/Issues/Defenders/Declaration/declaration_sp.pdf

en El Salvador, Guatemala, Honduras y/o Nicaragua, sin importar su género, edad, lugar de procedencia, antecedentes profesionales o de ningún otro tipo.

Por incidente entendemos cualquier evento adverso (verificado o en sospecha) relacionado con la información (incluyendo datos y metadatos) y/o comunicación digital.

Para que sea digital, esta información y/o comunicación debe haber sido creada, procesada y comunicada por los dispositivos electrónicos computacionales de la actualidad, y puede estar almacenada, puede estar siendo transmitida o puede encontrarse en un servicio en línea o en cualquiera de las aplicaciones que utilizamos para acceder a ellos (desde el correo electrónico hasta las redes sociales y los blogs y medios independientes en linea).

Cuando se identifica un incidente que no cumple con los criterios para ser registrado por el Observatorio, de todas formas Fundación Acceso brinda la atención técnica necesaria para asegurar la información digital que pudo haber sido comprometida, y si se tratara de un incidente de otra variable de la seguridad, ya sea física, legal o psicoscoal, se refiere el caso con organizaciones aliadas a nivel local y regional que trabajen ese tema en particular.

b) Tipología de incidentes

Los incidentes registrados se catalogan según la siguiente tipología

- Malware[3] o software malicioso: Cualquier tipo de software[4] que se ejecuta en los dispositivos para interrumpir las operaciones y recolectar información sensible sin consentimiento del usuario administrador. También se pueden instalar de manera oculta como complementos de algunos programas aparentemente legítimos, legales, sin mala fe o sin terceras u ocultas intenciones.

  Uno de los Malware más peligrosos es el conocido como spyware[5] o programa espía el cual recopila información almacenada en el dispositivo y la transmite a una entidad externa sin consentimiento del usuario administrador. Los programas instalados en celulares que realizan escuchas telefónicas, o activan vídeo y audio también son considerados Malware.

- Pérdida de hardware: Robo, hurto, destrucción, o extravío del equipo.

- Retención de hardware: Equipo incautado, confiscado y/o retenido por parte de agentes del Estado, con o sin orden legal, con o sin justificación legítima.

- Ataques remotos: Toma de control del equipo o extracción de información del mismo de forma remota, logrando el acceso mediante una conexión a internet o a una red. Los ataques remotos aprovechan vulnerabilidades del Módem[6] o del sistema operativo.

3. Techterms, Malware. Disponible en http://techterms.com/definition/malware.

4. Vamos a entender como Software como cualquier componente no tangible, por medio del cual se ejecutan determinadas instrucciones o rutinas que permiten utilizar un dispositivo.

5. Federal Trade Commission, Staff Report. Monitoring Software on Your PC: Spyware, Adware, and Other Software, (2005). Disponible en http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf

6. El Módem es el aparato proporcionado por el proveedor del servicio de internet. Convierte la información digital generada por las computadoras en frecuencias de sonido para ser transmitidas por una Red Telefónica, es decir, el aparato por medio del cual nuestras computadoras se conectan a internet.

7. La Red de Área Local (LAN, por sus siglas en inglés) se refiere al conjunto de computadoras ubicadas en un espacio determinado (como las oficinas de una organización), que pueden compartir archivos entre ellas y también pueden compartir salida internet.

•Ataques LAN[7]: Bloqueo del tráfico de datos que circula en la red local, interrupción de las conexiones entre las computadoras de la red, denegación de acceso a servicios y generación de tráfico en la red. Un ejemplo es el de reconfigurar los routers o modems para bloquear determinadas páginas.

•Ataques Web: Toda ataque a los servicios de internet que utilizamos y el monitoreo de los mismos. Estos pueden ser servicios de blogs o noticias, nuestros sitios web, bloqueo de nuestro canal de Youtube u otros, así como el monitoreo de nuestro comportamiento a partir de los sitios que visitamos.

Una de las principales técnicas informáticas para este tipo de ataque es DdoS (ataque de denegación de servicios), que es un ataque a la red que causa que un servicio o recurso sea inaccesible.

También se incluyen en esta categoría la censura de determinados sitios web por parte del Proveedor del Servicio de Internet, monitoreo de tráfico, robo de identidad en la web, suplantación de sitio web, aparición de publicaciones no autorizadas en el sitio web, cambios en el Servidor de Nombres de Dominio (DNS), inadecuada actualización y respaldo del sitio web.

•Compromiso de cuentas: Ésta es una categoría especial que debería estar contenida en "Ataques a Web" pero que, específicamente trata de craqueo de nuestras credenciales para acceder a los servicios que utilizamos. Se decide separar por la cantidad de incidentes de éste tipo que normalmente se dan[8].

Una de las principales técnicas informáticas para este ataque es el Phishing[9] o suplantación de identidad, caracterizado por intentar adquirir información confidencial de forma fraudulenta, particularmente las contraseñas de cualquier cuenta de correo electrónico, de suscripciones en Internet, de redes sociales, de administración de Hosting y sitios Web, cuentas bancarias, tarjetas de crédito, etc.

8. Recomendación de el equipo de Access Now a partir de su experiencia con el Help Desk.
9. Ed Skoudis, Phone phishing: The role of VoIP in phishing attacks.

Observatorio Centroamericano de Seguridad Digital

Momentos de Intervención:

Contacto Inicial 1

Ya sea por llamada telefónica, video-llamada, e-mail, mensaje de texto, mensajería instantánea, o personalmente. Se decide si puede o no ser un incidente, y si el/la técnico/a asistirá o no al lugar (1° Módulo del reporte)

2 **Verificación**

Técnico/a asiste al lugar para definir si efectivamente es un incidente o si es un falso positivo (2° Módulo del reporte)

Pre-diagnóstico 3

Si efectivamente es un incidente, se realiza una nueva visita al lugar con el/la abogado/a y se realiza un pre-diagnóstico, se define una estrategia (en conjunto con el/la defensor/a u organización de DDHH) y se decide si solo se registra o si es un posible caso jurídico (3° Módulo del reporte)

4 **Implementación de Estrategias**

Abogado/a y técnico/a realizan las acciones de la estrategia a la que se comprometieron durante la estrategia (4° Módulo del registro)

Peritaje Especializado 5

Abogado/a y técnico/a deciden si es necesario hacer un peritaje especializado para el que se necesita apoyo externo (Se agrega un 5° Módulo al registro con las acciones a tomar)

6 **Resultados Peritaje**

Resultados del peritaje (Se agrega un 6° Módulo al registro con los resultados del peritaje)

FUNDACIÓN Acceso

c) Contexto Nacional[10]

Acceso al mundo digital

Mientras una parte de la sociedad salvadoreña tiene la capacidad de acceder a los servicios tecnológicos de primer mundo, otro importante porcentaje de su población aún vive en situación de analfabetismo digital, siendo probablemente el acceso a la telefonía celular lo único que ambos mundos comparten en lo relativo a acceso al mundo digital. Para el año 2014 se calculaba que sólo un 30% de la población salvadoreña era usuaria de internet.[11]

Sin embargo, en 2014 se estimaba que había cerca de 1.8 millones de SmartPhones activos en el país, de un total de 9 millones de móviles registrados, número que supera la población total del país, que ronda los 6 millones de habitantes, según según datos contrastados del Organismo Especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación (UIT)[12] y del director país de la empresa Telefónica[13]. Los SmartPhones han posibilitado que, a pesar que la posesión de computadora y acceso al servicio de internet residencial sean aún bastante bajas, muchas personas en el país estén accediendo al mundo digital desde sus dispositivos móviles.

Sin duda, las nuevas dinámicas generadas por las tecnologías de la información han provocado que derechos como el de acceso a la información, libertad de expresión, libertad de prensa, derecho a la protección de datos y la privacidad, entre otros, se vuelven cada vez más importantes de discutir en la agenda pública de El Salvador [14].

En tal sentido, dado que en El Salvador ya se registraban para el año 2015 algunos testimonios de defensores y defensores que se enfrentaron a situaciones que pudiesen tratarse de ataques a su seguridad digital debido a su activismo[15], es de particular importancia para este proyecto profundizar sobre cuáles pueden ser aquellas acciones y entidades interesadas en afectar los entornos digitales de quienes se dedican a la defensa de los derechos humanos, así como conocer los mecanismos legales-institucionales y tecnológicos que pueden ser utilizados por las y los defensores de derechos humanos para protegerse.

10. Este apartado tiene como base el capítulo de El Salvador en la investigación Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos humanos?: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección,criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos (San José, Costa Rica: 2015). Disponible en http://acceso.or.cr/assets/files/Investigacion-Privacidad-Digital-FA.pdf

11. Dirección General de Estadísticas y Censos (2013). Resultados encuesta de hogares de propósitos múltiples 2013 (diapositivas). El Salvador: DIGESTYC. Recuperado de http://www.digestyc.gob.sv/index.php/servicios/descarga-de-documentos/category/47-presentaciones-estadisticas-sociales.html

12. Organismo Especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación - UIT. (2014). Informe sobre estadísticas de individuos que usan Internet en El Salvador.

Recuperado de: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

13. [El Diario de Hoy. 2014. Circulan 1.8 millones de smartphones en el país. El Diario de Hoy, 4 de noviembre, sección Negocios. http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=47861&idArt=9218924 (Fecha de consulta: 8 de abril de 2015).

14. Rafael Ibarra, “Gobernanza de internet” La Prensa Gráfica, http://blogs.laprensagrafica.com/litoibarra/?p=1205 (Fecha de consulta: 10 de marzo de 2015).

15. Fundación Acceso (2015), ¿Privacidad digital para defensores y defensoras de derechos?

Situación actual de defensoras y defensores de derechos humanos

La llegada del partido FMLN en 2009 al Ejecutivo significó un punto de inflexión para las personas y organizaciones defensoras de derechos humanos, dado que varios de sus cuadros asumieron cargos y responsabilidades públicas en los gobiernos del FMLN, pero también porque muchos de sus puntos importantes de agenda en defensa de los derechos humanos se enfrentaron con la diferencia que implica la agenda y las prioridades de un partido que fue aliado en la oposición, respecto de las agendas y prioridades de dicho partido en el ejercicio de gobierno.

Las acciones en materia de seguridad pública del segundo gobierno del FMLN, que inició en 2014, han puesto en una encrucijada importantes puntos de las agendas de algunas organizaciones y personas defensoras de derechos humanos, pues sus acciones en dicha materia área guardan mucha sintonía con los enfoques manoduristas de los gobiernos del partido ARENA.

En tal sentido, las y los defensores de derechos humanos actúan en un contexto marcado por la violencia criminal, pero también por un accionar cada vez más contradictorio con los derechos humanos y con el estado de derecho por parte de los cuerpos de seguridad estatal, en consonancia con el discurso anti-terrorista hacia las pandillas adoptado por el Gobierno de El Salvador en los últimos años. En este contexto, la seguridad física de cualquier persona es frágil, pero aún más las de aquellas que se dedican a la defensa de los derechos humanos.

En tal sentido, muchas de las personas defensoras con las que Fundación Acceso ha entablado relaciones, saben identificar momentos y acciones que podrían ser considerados como ataques o vulneraciones a su seguridad digital, identificándose una primaria noción sobre su seguridad digital, además de una inicial conciencia sobre la necesidad de proteger los aspectos relativos al mundo informático y digital, pero aún sin contar con las capacidades ni la mística para defenderse efectivamente de posibles ataques digitales.

Sin embargo, existe apertura de su parte para formarse en estos aspectos y adoptar prácticas y políticas institucionales/organizacionales tendientes a mejorar la seguridad de su entorno digital. El reto principal ahora se trata de la formación, disposición y priorización de los recursos para encaminarse hacia la creación y mantenimiento de entornos digitales más seguros.

1. PRINCIPALES HALLAZGOS EN EL SALVADOR

A continuación se presentan los principales hallazgos del Observatorio Centroamericano de Seguridad Digital para el caso de El Salvador. Los mismos han sido registrados entre los meses de junio y noviembre de 2016. Para el registro se elaboraron una serie de herramientas técnicas y legales para definir los criterios de registro de incidentes digitales.

1.1) Procedimiento para el registro de incidentes

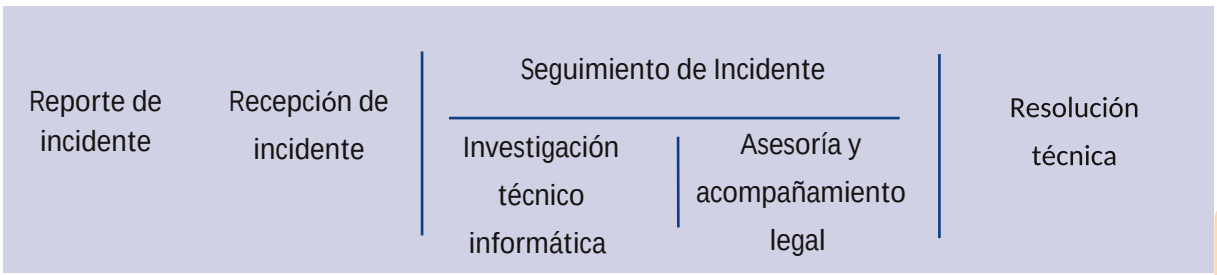
En el caso de El Salvador, el equipo estaba conformado por el asesor legal residente en el país y por dos técnicos residentes en Guatemala. Esto respondió al hecho de que Fundación Acceso, previamente, no había brindado asistencia técnica en El Salvador (como sí lo había hecho en Guatemala, Honduras y Nicaragua). Ante tal circunstancia se decidió que, de forma temporal, se cubriría la asistencia con los técnicos de Guatemala, quienes se trasladaron a El Salvador en 3 ocasiones, por un total de 12 días.

En estas visitas, las actividades consistían en visitar a organizaciones defensoras de derechos humanos de forma presencial para contarles sobre la iniciativa, presentar al equipo de trabajo, ofrecer asistencia técnica para seguridad digital, establecer planes de acción conjuntos, y posteriormente, para realizar el seguimiento de las acciones acordadas y de los incidentes reportados. Al mismo tiempo, estos espacios fueron aprovechados para comenzar a identificar personas residentes en El Salvador que, en un futuro, podrían brindar la asistencia técnica de Fundación Acceso en el país.

Luego de las reuniones con las organizaciones de derechos humanos, en las que manifestaban una diversidad de posibles ataques o dudas sobre incidentes sospechosos relativos a su seguridad digital, el equipo técnico-legal de Fundación Acceso brindada un seguimiento telefónico y virtual. Dicho seguimiento consistía principalmente en recordar a las organizaciones defensoras enviar sus reportes de posibles incidentes a los técnicos informáticos o bien, en recordar al equipo técnico del seguimiento que había que dar.

En algunas ocasiones, las llamadas o correos reportando incidentes fueron dirigidas al asesor legal. En estos casos el asesor legal reenviaba la información a los técnicos informáticos a través de correo electrónico y daba seguimiento vía mensajería instantánea con Signal.

En tal sentido pueden distinguirse los siguientes momentos de intervención:



Es importante tener en cuenta, que por diversos factores, ninguno de los casos reportados pasaron a las etapas finales de investigación técnica, por lo que nunca pudieron conocerse los posibles perpetradores ni tampoco se planteó la posibilidad de llevar los casos a etapas judiciales o previas a la judicialización.

1.2) Casos registrados

Para el caso de El Salvador es importante recordar que Fundación Acceso comenzó muy recientemente el trabajo en terreno en el país (siendo un antecedente importante la investigación sobre derecho a la privacidad digital realizada en el año 2015) y el consiguiente fortalecimiento de relaciones de confianza con personas defensoras de derechos humanos. Si a esto sumamos el hecho de que el equipo técnico aún no tiene permanencia constante en el país y la dificultad de muchas de las entidades de contar con un técnico informático permanente o estable (sólo una de ellas cuenta con uno exclusivo y a tiempo completo), los casos a los que se les dio seguimiento y registro de manera más consistente fueron relativamente pocos.

Las entidades que informaron sobre incidentes fueron cuatro, dedicadas principalmente a la defensa de derechos de la mujer, derechos LGBTI, jóvenes en riesgo y desempeño de instituciones de seguridad pública, entre otras áreas de derechos humanos que también desarrollan algunas de ellas. Todas tienen su sede y trabajo en el departamento de San Salvador, pero un par de ellas desarrollan trabajo y tienen presencia también fuera de este departamento.

En algunos de los casos las entidades manifestaban más de un tipo de ataque, sin embargo, dado que la asesoría y pericia técnica debía darse a la distancia, se eligieron los casos que podrían ser más factibles para darse remotamente.

a) Perfil de las personas/ organizaciones que reportaron incidentes

Organizaciones y personas defensoras de derechos humanos, principalmente trabajando en aspectos relativos a seguridad pública. Tres de las entidades que reportaron incidentes (dos organizaciones y una persona defensora de derechos humanos) se encuentran vinculadas a temas de seguridad pública, bien porque trabajan con jóvenes en riesgo de violencia y en conflicto con la ley, o porque registran y/o brindan algún tipo de acompañamiento a víctimas de violaciones de derechos humanos de parte de agentes vinculados a los servicios de defensa y seguridad pública del Estado. Así también, es importante mencionar que según las entidades defensoras de derechos humanos -en tres de los casos- los ataques reportados se dieron en el marco de acciones visibles de defensa de derechos humanos (campañas, informes, casos judicializados).

b) Tipos de ataques

A continuación una breve descripción (no técnica) de los ataques registrados.

Ataque 1

El sitio web de una de las organizaciones defensoras de derechos humanos fue vulnerado, haciendo que las y los usuarios de la misma fueran redirigidos automáticamente a una página pornográfica, resultando imposible acceder a la información oficial de la institución.

Ataque 2

El teléfono celular de una entidad defensora de derechos humanos se desconfiguró y posteriormente se dañó, apenas unas horas luego que la persona defensora usuaria del teléfono participara en manifestaciones contra una institución pública.

Ataque 3

Durante una campaña lanzada por una entidad defensora de derechos humanos, el sitio web de la campaña es atacado de manera que se vuelve inaccesible para los usuarios de la misma.

Ataque 4

Apenas unos días después de presentar su sitio web recientemente creado, la entidad defensora de derechos humanos es objeto de ataques que logran inhabilitarlo.

c) Posibles perpetradores

La identificación de los posibles perpetradores de los ataques es una tarea que interesa al Observatorio de Seguridad Digital, pero debemos informar que no siempre se logra porque un atacante regularmente tratará de anonimizarse y para ello utilizará los recursos técnicos y metodológicos que convengan para el tipo de ataque. En tal sentido, esta tarea requiere, para los casos más complejos, recursos técnicos y acceso a servicios que están fuera de nuestro alcance. No obstante lo anterior, sobre la base de los hallazgos de los ataques se puede delinear un posible perfil técnico del atacante y sus objetivos.

Por diversos factores, desde las limitaciones técnicas hasta los de recursos o por las decisiones de las entidades, en ninguno de los casos, los peritajes técnicos realizados llegaron hasta la etapa de buscar posibles perpetradores.

Es necesario entender además que todos los sitios web alojados en internet están sometidos a ataques de forma permanente, estos son realizados por piratas informáticos que buscan incrementar popularidad en internet, en estos casos los sitios web que tienen poco o nulo mantenimiento suelen ser víctimas de estos ataques, en los casos descritos anteriormente pudimos observar éste tipo de comportamiento.

2. MECANISMOS DE PROTECCIÓN

En este apartado se presentan los marcos jurídicos que pudieron haber sido vulnerados en los casos que se han registrado en el capítulo de El Salvador del Observatorio Centroamericano de Seguridad Digital. De igual forma se analizan cuáles son las posibles estrategias que estos casos permiten llevar adelante en función de promover los derechos digitales de las personas defensoras de derechos humanos.

En El Salvador, el 6 de marzo de 2016, entró en vigencia la Ley Especial contra los Delitos Informáticos y Conexos (LEDI), a partir de la cual haremos principalmente las valoraciones y recomendaciones de mecanismos jurídicos de protección. Hasta antes de esta ley, lo relativo a delitos informáticos se encontraba de forma fragmentada en algunas leyes cuyo objetivo principal no eran los delitos informáticos, como por ejemplo, el código penal o ley de protección al consumidor. En tal sentido, la LEDI profundiza y cohesiona lo relativo a delitos informáticos, por lo que dada su particularidad, al ser una ley especial, según el ordenamiento jurídico salvadoreño deberá ser la legislación que prime en caso de entablarse alguna contienda judicial relativa a seguridad digital o informática.

2.1) Violaciones de derechos

a) Posibles Derechos fundamentales/humanos vulnerados

Dada la naturaleza de los ataques registrados, los principales derechos humanos violentados son el derecho a la identidad, la intimidad e imagen, y la propiedad, de las personas y organizaciones defensoras de derechos humanos, según lo establecen la LEDI en su artículo 2 y la Constitución de la República en su artículo 2 que reconoce el derecho al honor, a la intimidad personal y familiar, y a la propia imagen. El mismo artículo a la Constitución también reconoce el derecho a la propiedad y posesión.

Así también, el derecho a la libertad de expresión podría tomarse como uno de los posibles derechos vulnerados, pues tomando en cuenta el contexto de algunos de los ataques registrados, cabe la probabilidad que tuviesen como intención afectar la capacidad y posibilidad de expresar las posturas y planteamientos de las entidades defensoras de derechos humanos.

b) Posibles Tipificaciones penales

Es importante tener en cuenta que las valoraciones jurídicas de los tipos penales contenidos en la LEDI, en caso de llegarse a etapas de judicialización, deberán contar con el respectivo contraste y soporte técnico informático, ya que la adjudicación de un tipo ideal de delitos a cierta hecho o conducta, estará mediatizada por la valoración/interpretación técnica informática que se haga de estos durante el proceso judicial o pre-judicial (sede fiscal). Es decir que, la adjudicación de los tipos ideales penales dependerá, más que en cualquier otro tipo de casos, de una lectura altamente especializada de los hechos, la cual, además, es de compleja o difícil compresión para las personas que no tienen entrenamiento en estos aspectos (como pueden ser los fiscales, defensores o jueces).

Teniendo en cuenta esa acotación inicial, uno de los delitos que podrían configurarse a partir de los ataques registrados a las páginas web de las organizaciones defensoras es el de Hurto de Identidad (Art. 22 LEDI), según el cual aquél que suplante o se apodere de la identidad de una persona natural o jurídica por medio de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de tres a cinco años.

Por otra parte, de manera conexa, en el caso del ataque a la página web institucional que era redireccionada a un sitio web pornográfico, podrían configurarse los delitos de pornografía contemplados en el Código Penal (Arts. 172, 173, 173A y 173B) en caso de comprobarse que se utilizó a menores de edad en la pornografía o que hubo menores de edad expuestos ante este material pornográfico.

c) Posibles infracciones civiles

El artículo 2 de la Constitución también establece que toda persona tiene derecho a la integridad moral, y se reconoce la indemnización por daños de carácter moral. En tal sentido, además del juicio penal, queda abierta la posibilidad de la reparación de daños por la vía civil en caso de comprobado daño a su imagen (identidad), intimidad o propiedad. La LEDI también contempla esta posibilidad, aunque no menciona taxativamente las posibles infracciones civiles, sino que remite a las legislaciones respectivas:

> Las sanciones previstas en la presente Ley, serán aplicables sin perjuicio de otras responsabilidades penales, civiles o administrativas en que se incurra. Para la deducción de la responsabilidad civil se estará a lo dispuesto en la normativa aplicable (Art. 35).

Sin embargo, por datar de 1859, el Código Civil salvadoreño no contempla muchas de las circunstancias que podrían configurarse en materia de seguridad digital, además de no contemplar muchos aspectos que la Constitución o las leyes secundarias vigentes sí contemplan respecto al derecho a la intimidad, libertad de expresión o propia imagen (identidad).

Por lo anteriormente expuesto se requiere de esfuerzos importantes de interpretación e integración jurídica por parte de los jueces y de los fiscales. Por ejemplo, según lo establecido en el artículo 2082 del Código Civil respecto a "las imputaciones injuriosas contra el honor o el crédito de una persona no dan derecho para demandar una indemnización pecuniaria, a menos de probarse daño emergente o lucro cesante, que pueda apreciarse en dinero", podría interpretarse que las imputaciones injuriosas contra el honor o el crédito de una persona, son equivalentes a los derechos a la intimidad, el honor y la propia imagen, que contemplan la Constitución de la república y la LEDI.

2.2) Estrategias de respuesta

a) Legales

- En materia penal

Las denuncias en materia penal son una opción legal importante luego de la aprobación de la LEDI, en marzo de 2016. En el caso de El Salvador, el monopolio de la Acción Penal recae sobre la Fiscalía General de la República (FGR), por lo que las denuncias deberán ser interpuestas ante este órgano del Estado. Sin embargo, a pesar de las facultades legales que le confiere la ley y la Constitución, las capacidades técnicas de la FGR tanto en lo jurídico como en lo informático muy probablemente aún no son compatibles con los constantes cambios y la tecnificación del mundo informático y digital.

Además, debe tomarse en cuenta que según la investigación de Fundación Acceso sobre privacidad y vigilancia de personas defensoras de derechos humanos (2015), las personas defensoras de derechos humanos manifestaron no tener mayor confianza en dicha FGR, sino al contrario, la consideran como una entidad pública que les brinda poca confianza y les despierta muchos resquemores.

16. Sentencia de Amparo 934-2007 de la Sala de lo Constitucional de la Corte Suprema de Justicia, San Salvador, de fecha 4 de marzo de 2011. Parte III 1. B. a.

•En materia constitucional

El recurso de Amparo ha sido habilitado como un supletorio del Habeas Data según la jurisprudencia constitucional salvadoreña, la cual estableció que mientras no se cuente con una legislación secundaria ad hoc, podrá ser utilizado para la protección de datos personales[16]. Sin embargo, de los casos registrados por el Observatorio, no puede distinguirse claramente una afectación directa a los datos de personas defensoras de derechos humanos. Sin embargo, esto podría ser una posibilidad si las pericias técnicas mostraran evidencias de posibles injerencias en los datos personales de algunas organizaciones de derechos humanos.

En el caso del marco jurídico salvadoreño, el recurso de Amparo se interpone ante la Sala de lo Constitucional de la Corte Suprema de Justicia, que es el máximo tribunal en materia constitucional. Lastimosamente, los recursos en materia constitucional necesitan de una alta formación jurídica y no son accesibles para cualquier persona.

•Vías Administrativos y de otra índole

Procuraduría para la Defensa de los Derechos Humanos (PPDH)

A pesar que ninguno de los incidentes registrados llegó hasta la etapa de arrojar posibles perpetradores, es importante plantear algunas estrategias legales que de manera general podrían ser útiles en hipotéticos incidentes de seguridad digital. En el caso del incidente del teléfono que sufrió daños en su sistema luego que su portador participara en una protesta contra una entidad pública, además de la denuncia ante la FGR amparándose en LEDI, sería importante la interposición de la denuncia ante la Procuraduría para la Defensa de los Derechos Humanos (PDDH), ya que ésta tiene las facultades legales para solicitar informes sobre el Centro de Intervención de Telecomunicaciones, a cargo de la FGR, en caso de un posible uso indebido de sus facultades para intervenir las telecomunicaciones de personas que se presume son parte del crimen organizado. Por tratarse posible incidente que implica un daño al software del teléfono móvil, deberá cubrirse la posibilidad que no se trate de una intervención indebida o ilegal, por lo que resulta importante la utilización de la PDDH.

17. Resolución 128-UAIP-FGR-2015 a Solicitud de Acceso a la Información presentada por el investigador el 24 de julio de 2015.

18. Fundación Acceso, 2015. ¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección,criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. San José, Costa Rica.

Instituto de Acceso a la Información Pública (IAIP)

Por otra parte, según el artículo 31 de la Ley especial para la Intervención de las Telecomunicaciones (LEIT), el funcionamiento y seguridad del Centro de Intervenciones a las Telecomunicación, así como la selección y fiscalización permanente, tanto del Director, funcionarios, personal y miembros de la Policía Nacional Civil (PNC) que labore en el mismo, estará normado en un reglamento que para tal efecto deberá elaborar el Fiscal General. Sin embargo, este reglamento no es público, pues según el criterio de la Unidad de Acceso a la Información Pública (UAIP) de la Fiscalía esta normativa se encuentra clasificada como Información Reservada.[17] Sin embargo, tanto la normativa interna como los principios internacionales establecen que las leyes, reglamentos, decretos y demás disposiciones de carácter general sólo tendrán fuerza obligatoria en virtud de su promulgación y publicación [18].

Por tal razón y de manera general, se sugiere inicialmente una estrategia a través de la vía administrativa, por medio de la interposición de una solicitud de acceso a la información nuevamente ante la Fiscalía General de la República (FGR), para que en caso de negativa se apele ante el Instituto de Acceso a al Información Pública (IAIP). Posteriormente, en caso que la ruta administrativa no fuese fructífera, podría seguirse la ruta judicial, a través de la interposición de un recurso de Amparo ante la Sala de lo Constitucional.

b) No legales

Otras estrategias de respuesta, de índole político, podrían ser las medidas de persuasión, incidencia o presión para que la FGR haga pública la información oficiosa respecto al Centro de Intervención a las Telecomunicaciones, es decir, aquella que pueda y deba ser revelada, como la cantidad de intervenciones realizadas en un año, las que siguen en curso y las que ya finalizaron, los tipos de delitos por los que están siendo intervenidos, entre otra información que sea pertinente y que no afecte el proceso penal de investigación respectivo.

De igual manera se sugieren acciones de incidencia pero también de capacitación técnica para que la PDDH pueda desempeñar las funciones de control sobre el Centro de Intervenciones que la Ley especial para la Intervención de las Telecomunicaciones (LEIT) le faculta, pues hasta el momento dicha institución no está cumpliendo con dicha función de verificar el respeto a la legalidad y los derechos humanos en los procedimiento de intervención a las telecomunicaciones, siendo un procedimiento, que de no ser controlado eficazmente, puede devenir en una grave y masiva situación de vigilancia y hostigamiento hacia defensores de derechos humanos y opositores políticos, según los intereses o criterios del fiscal general de turno.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Desde el trabajo técnico-digital se puede aseverar que los ataques a los sitios web se concretaron teniendo los resultados que se apuntaron en la descripción de los mismos. En el caso del teléfono celular, debido a que no se tuvo acceso al mismo, no se puede aseverar que haya sido objeto de algún ataque, en todo caso, lo único que podemos señalar es la sospecha de ataque, puesto que se enmarca en un contexto de fuerte activismo de parte de los usuarios del aparato.

En lo que respecta a la identificación de los objetivos y la individualización de los perpetradores de los ataques, el Observatorio en Seguridad Digital idealmente debe proporcionar información verificable para sostener cualquier señalamiento. En ninguno de los cuatro casos tenemos pruebas contundentes que permitan determinar objetivos y atacantes, pero ello no implica que no hayan ocurrido los ataques. Verificamos en uno de los casos la existencia de serias vulnerabilidades en el servicio de Hospedaje y en los programas utilizados para el manejo del sitio, los cuales fueron explotadas por los atacantes. No se pudieron individualizar a los atacantes, pero los indicios apuntan a la intervención externa de personas no autorizadas para alterar los sitios web analizados, es decir, no se puede negar el ataque.

Aunque en uno de los casos se utilizó uno de los sitios para promocionar contenido pornográfico, no tenemos elementos que nos permitan señalar fehacientemente que el propósito del ataque haya sido precisamente la facilitación de los mencionados contenidos, y del mismo modo tampoco podemos aseverar que el propósito del ataque fue deslegitimar o desprestigiar a la organización, pero tampoco podemos descartarlo.

Después de revisar los sitios web de la organizaciones que reportaron incidentes, además de sitios de otras organizaciones con las que hemos trabajado, resulta evidente que los sitios web carecen de los estándares básicos de seguridad, que permitan a los sitios mantenerse limpios, esto coloca en una situación bastante delicada a las organizaciones y sus contenidos digitales.

Recomendaciones

Entre las lecciones aprendidas para el caso de El Salvador se encuentra la necesidad que tienen las organizaciones y personas defensoras de contar con un acompañamiento técnico de manera constante y que la persona que cumpla este rol se encuentre formada y actualizada respecto de los

estándares de seguridad digital, pues con excepción de una de las entidades, el resto no posee un técnico estable ni la capacitación suficiente en aspectos de seguridad digital. Este es un aspecto importante a fortalecer de las organizaciones y personas defensoras de derechos humanos en El Salvador, en las que sin duda Fundación Acceso podría hacer una diferencia aún mayor.

Hasta este momento, el nivel de sensibilidad sobre la seguridad digital a nivel de cargos de decisión en las organizaciones defensoras de derechos humanos es bastante bueno, mejorando significativamente respecto a 2015, cuando Fundación Acceso realizó la investigación sobre privacidad y vigilancia digital. Existe apertura, interés y, en algunos casos, ya se han comenzado a implementar decisiones iniciales respecto a seguridad digital. Es importante destacar que la única entidad con la que trabajamos que cuenta con un técnico informático más estable, es la que logró aprovechar aún mejor las capacitaciones y capacidades del equipo de Acceso, pero también con quien pudimos llegar más adelante en el proceso de registro del Observatorio.

Para el caso de El Salvador es de vital importancia buscar y formar personas técnicas informáticas ligadas a derechos humanos y, de ser posible, formar una red con ellas, para que las entidades y personas defensoras de derechos humanos puedan contar con una mejor seguridad digital.

Entre las lecciones aprendidas, también puede mencionarse la necesidad de contar con formatos sencillos, lo suficientemente comprensibles para personas no técnicas en informática, para que puedan hacer reportes iniciales de los que consideran posibles ataques a su seguridad digital. Así también, generar boletines u otro de tipo de información que ilustre y ejemplifique de manera relativamente sencilla algunos incidentes digitales, para que las y los defensores puedan tener mayor claridad de cuándo podrían estar ante uno de ellos.

Por otra parte, para que el registro de incidentes en el Observatorio sea más efectivo es altamente recomendable contar con un técnico de Fundación Acceso sólo para el registro de incidentes de El Salvador y, en la medida de lo posible, destacado en el país o con facilidad para viajar frecuentemente. Esto debido a que, al no estar físicamente disponible se hace más difícil el registro para ciertos casos en los que se necesite intervenir o resguardar físicamente algunos dispositivos. Este es, por ejemplo, el caso de un teléfono celular o una computadora, los cuales no pueden esperar semanas o meses sin tocarse hasta que el técnico llegue a revisarla luego de sucedido el incidente.

BIBLIOGRAFÍA

Legislación nacional

•CC. Código Civil. 1859. El Salvador: Asamblea Legislativa.

•CN. Ver Constitución de la República de El Salvador. 1983. El Salvador: Asamblea Legislativa.

•CP. Ver Código Penal. 1997. El Salvador: Asamblea Legislativa.

•CPP. Ver Código Procesal Penal. 2009. El Salvador: Asamblea Legislativa.

•LAIP. Ver Ley de Acceso a la Información Pública. 2012. El Salvador: Asamblea Legislativa.

•LEIT. Ver Ley Especial para la Intervención de las Telecomunicaciones. 2010. El Salvador: Asamblea Legislativa.

•LEDI. Ver Ley Especial contra los Delitos Informáticos y Conexos. 2016. El Salvador: Asamblea Legislativa.

Jurisprudencia

•Sentencia de Amparo 934-2007 de la Sala de lo Constitucional de la Corte Suprema de Justicia, San Salvador, de fecha 4 de marzo de 2011. Parte III, 1 A.

•Sentencia de Amparo 934-2007 de la Sala de lo Constitucional de la Corte Suprema de Justicia, San Salvador, de fecha 4 de marzo de 2011. Parte III 1. B. a.

Otros documentos

•Fundación Acceso, 2015. ¿Privacidad digital para defensores y defensoras de derechos humanos?: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección,criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. San José, Costa Rica.

•Dirección General de Estadísticas y Censos (2013). Resultados encuesta de hogares de propósitos múltiples 2013 (diapositivas). El Salvador: DIGESTYC. Recuperado de http://www.digestyc.gob.sv/index.php/servicios/descarga-de-documentos/category/47-presentaciones-estadisticas-sociales.html

•El Diario de Hoy (2014). Circulan 1.8 millones de smartphones en el país. El Diario de Hoy, 4 de noviembre, sección Negocios.

•http://www.elsalvador.com/mwedh/nota/nota_completa.aspidCat=47861&idArt=9218924 Fecha de consulta: 8 de abril de 2015.

•Organismo Especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación - UIT. (2014). Informe sobre estadísticas de individuos que usan Internet en El Salvador.
Recuperado de: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

•Organismo Especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación - UIT. (2014). Informe sobre estadísticas de individuos que usan Internet en El Salvador. Recuperado de: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

•Rafael Ibarra (2015), "Gobernanza de internet" La Prensa Gráfica, http://blogs.laprensagrafica.com/litoibarra/?p=1205 (Fecha de consulta: 10 de marzo).

ioxwxvU

Eb

HlqVRomqggh

j86Z/sIDhll vy5

j86Z/sIDhll vy5Wvrrsk

FUNDACIÓN Acceso