No.16 / enero-febrero 2013 ISSN: 1251478, 1251477

.Seguridad

Cultura de prevención para TI

16

Imagen y reputación

Presencia virtual en construcción

CERTS | Reputación línea | Politicas seguridad | Riesgo reputacional | WAF | Mando tecnólogico

Contenido

.Seguridad
Cultura de prevención para TI

Editorial

Imagen y reputación
Presencia virtual en construcción

Imagina las fases del proceso de construcción de un edificio, desde el diseño, la planeación, el listado de todos los requerimientos, el largo proceso de cimentación y finalmente, la obra terminada. Es un trabajo arduo, aunque trae consigo firmeza, estabilidad y protección.

De esta misma forma queremos que imagines el proceso de edificación de tu imagen en línea, como un gran proyecto de diseño e implementación. El proceso es largo, a veces complicado y requiere echar mano de muchos elementos, no solo materiales, sino humanos y de esfuerzo mismo. Incluso cuando está terminado, nuestra gran obra requiere de constante cuidado y mantenimiento. Aunque afanosas, estas atenciones diarias nos mantienen en el entorno de la tranquilidad.

El laborioso camino de la construcción y cuidado de nuestra reputación digital es un esfuerzo constante y, debido a esto, buscamos ofrecerte con esta edición, esas herramientas, materiales y mano de obra que necesitas todos los días para la gran tarea de pulir tu presencia virtual.

Esta entrega, particularmente especial para nosotros, cuenta con la participación de grandes expertos reconocidos a nivel internacional, lanzamos nuestra edición conmemorativa de 4 años de arduo trabajo con personalidades como Eduardo Carozo y Jesús Torrecillas, también contamos con la colaboración muy especial de Raúl Ortega, pilar entrañable en la historia de esta revista.

Esperamos que este número sea realmente útil para ti y que con su lectura, logres sumar un ladrillo más al constante proceso de construcción de tu imagen virtual. Con toda sinceridad te decimos ¡Muchas gracias! y te esperamos como siempre, en nuestras próximas ediciones.

L.C.S Jazmín López Sánchez
Editora
Subdirección de Seguridad de la Información

.Seguridad
Cultura de prevención para TI

.Seguridad Cultura de prevención TI M.R. / Número 16 / Enero - Febrero 2013 / ISSN No. 1251478, 1251477 / Revista Bimestral, Registro de Marca 129829

Centro de respuesta a incidentes informáticos… ¿Para qué?

Eduardo Carozo Blumsztein

Es sorprendente ver cómo la tecnología de la información se incorpora cada vez más a nuestras vidas, inclusive atravesando la última frontera. Algunas de las prestaciones de dispositivos, aplicaciones y sistemas de mayor desarrollo en la actualidad ingresan al interior de nuestro cuerpo con singular éxito: sondas, marcapasos, microelectrónica aplicada para la asistencia a personas con discapacidades auditivas o visuales, localización permanente de personas...

Ese mismo nivel de interacción se observa en las organizaciones, donde ha aumentado radicalmente la facilidad de acceso a las redes con múltiples dispositivos que, además, son multifuncionales. Un teléfono que puede convertirse en Access Point Wi-Fi es algo absolutamente común en nuestros días, así como conexiones USB utilizadas para múltiples dispositivos, etc. Lo único que falta, es inventar discos duros que se parezcan a adornos en los dientes, porque creo que todo lo demás ¡está inventado! (en los lentes, con formas de juguetes, etc.). Si bien parece divertido, a la hora de asegurar la información, toda esta situación genera grandes dificultades y desafíos.

En la medida que los servicios de TI y los dispositivos se hacen más baratos, cercanos, difundidos y omnipresentes, la carencia o mal funcionamiento de alguno de ellos provoca impactos más altos y masivos.

Por ejemplo, los sistemas de prepago de celulares involucran a millones de personas y son lo suficientemente complejos como para tener interrupciones o demoras de forma periódica, siendo en general compleja la recuperación de los servicios.

¿Cuánto demora una comunidad de clientes de prepago en saber que el sistema está caído y (en algunas compañías) puede hablar sin límite? Es cuestión de segundos o minutos ¿Cuánto dinero e imagen pierde la compañía?, bastante. Lo peor es que estas pérdidas van en rápido ascenso debido a la masificación de los servicios.

Así podemos enumerar múltiples servicios que hoy son indispensables, como la banca en línea, el voto electrónico, la venta de servicios y productos online, además de otros con los que convivimos a diario y que, bajo un incidente, podrían sufrir una interrupción inesperada. Este hecho impacta en forma cada vez más relevante las finanzas o reputación de las organizaciones involucradas.

Para dar este tipo de servicios, la complejidad de los equipamientos, redes y administradores de sistemas ha aumentado exponencialmente, por lo que diagnosticar la causa de una interrupción en un proceso de TI se está volviendo cada vez más complejo.

Existen miles de sistemas operativos, miles de protocolos y miles de formas de configurar las redes e intercambiar datos, además de millones de aplicaciones interactuando. Entonces, esto termina en infinidad de asuntos que atender a la hora de diseñar un nuevo proceso; y otras tantas causas de problemas a la hora de resolver un incidente.

La complejidad existente detrás de un servicio provoca en ocasiones, que frente a una alarma de incidente, distintos operadores de los diversos sistemas que lo soportan comiencen a promover cambios en aras de recuperar el servicio. Lejos de mejorar la situación, la vuelven irreversible, por lo que se ha constatado que es necesario coordinar las acciones de respuesta frente a un incidente de cualquier tipo para lograr una efectiva resolución del problema.

Por otro lado, la mayor parte de los usuarios de TI tienen un alto grado de desconocimiento del tipo de incidentes de seguridad más comunes, por lo que adoptan conductas inadecuadas en el uso de los dispositivos o servicios, colaborando frecuentemente con el éxito de los ataques.

Así las cosas, el proceso de seguridad de la información debe ser atendido y entendido por los directivos, sobre todo si la organización es usuaria intensa de las tecnologías de la información.

¿Qué es un Centro de Respuesta a Incidentes Informáticos?

Un Centro de Respuesta a Incidentes de Seguridad Computacionales (CSIRT) es un equipo de técnicos especialmente entrenados para resolver y gestionar incidentes informáticos de alto impacto. Dicho entrenamiento provee capacidades al mencionado equipo para gestionar crisis, coordinar acciones, estar preparado para prevenir y detectar los ataques cibernéticos más comunes, así como para conocer profundamente las debilidades de sistemas, infraestructuras y personas de su organización. El objetivo es dar una efectiva y rápida respuesta a los incidentes que puedan ocurrir.

Dicho equipo es muy parecido a una brigada de bomberos, ellos deben entrenar en forma continua para poder controlar rápidamente los incidentes más comunes. Cuanto más rápidamente mitiguen al incidente, menos impacto sufrirá la organización.

Es frecuente encontrarse con sistemas que facturan más de cincuenta mil dólares por hora. Contar o no con una respuesta acertada provoca bajar la discontinuidad de la operación en el orden de 10 horas promedio por incidente, por lo que la velocidad de la respuesta de recuperación se vuelve crucial.

Un CSIRT bien diseñado se encarga de proteger las infraestructuras críticas de la organización y vela por la continuidad de los servicios principales de la misma.

Existen diferentes tipologías de centros de respuesta que permiten adaptar y mejorar el desempeño de dichos grupos, según se encuentre alojado en una universidad, empresa, gobierno u organización internacional. Dichas tipologías están fuertemente vinculadas con la misión de la organización (sobre todo en términos de autoridad y funciones), además de la dispersión geográfica de la misma.

Vinculación entre un SGSI y un CSIRT

Un SGSI es un Sistema de Gestión de Seguridad de la Información y un CSIRT, como lo hemos dicho, es un Centro de Respuesta a Incidentes de Seguridad Informática, según sus siglas en inglés.

Uno de los principales problemas que un buen desempeño en la respuesta a incidentes desafía, es la existencia de una adecuada cultura de prevención y cuidado de los activos de información difundida entre los integrantes de la organización.

Para ello, dichos activos deben estar correctamente identificados, las personas que manejan dicha información deben estar

suficientemente sensibilizadas y capacitadas sobre los riesgos inherentes a manipular los activos y, en general, debe haber un buen manejo (preventivo) de los sistemas, infraestructura y dispositivos en torno a dicha información.

Es frecuente encontrarse en las organizaciones con funcionarios indiferentes respecto a la seguridad informática que promueven conductas inadecuadas, por ejemplo, con respecto a los privilegios de sus cuentas de usuario ¡Todos quieren ser administradores! En la mayoría de los casos sin siquiera conocer los riesgos asociados a dicha condición.

Por otra parte, es necesario que esté claramente definida la política de seguridad de la información para poder discernir qué es un incidente de seguridad y qué no lo es. En ciertos ambientes, un port-scanning no es un incidente y en otros es un incidente gravísimo, eso debe ser claramente establecido por la política de seguridad de la información y normas asociadas.

En resumen, tener un SGSI definido da el marco normativo necesario para una acción efectiva del CSIRT, promueve una cultura de seguridad, sensibiliza y alerta a los funcionarios de la organización acerca de qué es un incidente de seguridad. Antes de implementar el CSIRT, se recomienda desarrollar o fortalecer el programa de seguridad de la información de la organización.

Tener un SGSI sin disponer de un CSIRT que responda a los incidentes es ineficiente y frustrante, es similar a tener leyes de conducta ciudadana sin que existan policías o bomberos para desestimular, desactivar, mitigar o reprimir los incidentes. El sistema detecta la existencia del incidente, pero la organización no podrá dar una respuesta coordinada y efectiva.

Por otra parte, la gestión del conocimiento es totalmente inefectiva, puesto que en cada incidente se deberá crear nueva experiencia porque no existe ningún sitio en la organización que acumule y gestione el conocimiento propio o ajeno en la resolución de los incidentes previos, lo que provoca demoras y falta de asertividad en la recuperación.

Una visión directiva de la implantación (beneficios y esfuerzos)

Disponer de un centro de respuesta brinda a los directivos de una organización los siguientes beneficios:

-Un punto de contacto focal reconocido y confiable dentro de la organización para la denuncia y gestión de los incidentes.
-Promover la utilización de la infraestructura informática bajo buenas y mejores prácticas.
-Disponer de un equipo especializado y asesor para la protección de los nuevos desarrollos, basado en tecnologías no conocidas.
-Brindar información en tiempo real a toda la organización sobre vulnerabilidades, asociar y promover sus respectivas recomendaciones en forma más asertiva, además de mejorar significativamente su mitigación y/o control.
-Proveer servicios de publicación de información difundiendo la cultura de seguridad informática.
-Conocer, participar y compartir las experiencias de equipos similares estableciendo y haciendo propias las mejores estrategias para el manejo efectivo de incidentes de seguridad informática en la organización.
-Administrar puntos de contacto con otros CSIRT para promover alertas tempranas de ataques que están siendo exitosos en otros entornos u organizaciones.
-Poseer un equipo de personal especializado en constante proceso de actualización con la intención de brindar servicios de soporte informático.

Respecto a los esfuerzos necesarios, un CSIRT habitualmente se compone de pocos funcionarios bien entrenados (una estimación reciente establece un funcionario CSIRT en cada ochocientos puestos en organizaciones medias), con presupuestos anuales en general menores a los diez mil dólares por funcionario, excluyendo

salarios. Con el costo evitado, la inversión inicial se recupera en menos de un año y los costes operativos son cubiertos al tercer incidente resuelto en forma efectiva en dicho año.

Un esfuerzo importante que debe considerarse es el apoyo a este equipo desde la dirección de la organización, promoviendo y cuidando que no sea excluido por sus pares de los equipos técnicos.

Ocasionalmente y debido a problemas de inserción derivados de la falta de comunicación, los técnicos del CSIRT son visualizados por el resto de los gestores de TI como un grupo de élite que oficia de auditor, juzgando el accionar de los demás con altos privilegios en la organización. Promover esta imagen es un error, indirectamente promueve que los operadores del sistema de información que están siendo objeto de un ataque o que tienen un problema operativo serio, intenten ocultar el incidente por temor a los informes o represalias que puedan ocurrir si el incidente se hace público en la organización, en vez de recurrir a la ayuda de su centro de respuesta.

La dirección y los integrantes del centro de respuesta, en consecuencia, deberían promover activamente una función de auxilio y apoyo a los demás actores técnicos de la organización (al igual que un cuerpo de bomberos) y ponerse al servicio de su comunidad minimizando conductas competitivas o agresivas de los interlocutores.

La frase que sigue pertenece a un amigo director de una gran organización, consultado respecto del funcionamiento de su CSIRT, considero que puede constituir un excelente cierre para este artículo.

“Tener un centro de respuesta es una excelente solución para entender las TI de mi organización, obteniendo respuestas de un tercer actor independiente, capaz y objetivo. Recuerdo cuando uno de los muchachos de la división informática había sido víctima de un ataque que comprometió nuestros servicios en línea. Para esa persona, el soporte del CSIRT fue fundamental porque demostró que él no fue culpable de nada, sino que fue atacado y que nada podía hacer, más que avisar. Gracias a su aviso y a una respuesta adecuada, salvamos un par de millones y pudimos detectar a los responsables del ataque y su móvil de actuación.
Él no tuvo consecuencias en su carrera funcional, en definitiva evitamos un montón de costos humanos y materiales, el incidente no se ha vuelto a repetir”.

www.cert.org
www.proyectoamparo.net

[1] El término port-scanning, en español escáner de puertos, se emplea para designar la acción de analizar, por medio de un programa, el estado de los puertos de una máquina conectada a través de una red de comunicaciones. Detecta si un puerto está abierto, cerrado o protegido por un cortafuegos o firewall. Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos. Es usado por administradores de sistemas para analizar posibles problemas de seguridad, pero también es utilizado por usuarios malintencionados que intentan comprometer la seguridad de la máquina o la red. Existen varios programas escaneadores de puertos por la red. Uno de los más conocidos es Nmap, disponible tanto para Linux como Windows.

Reputación en línea

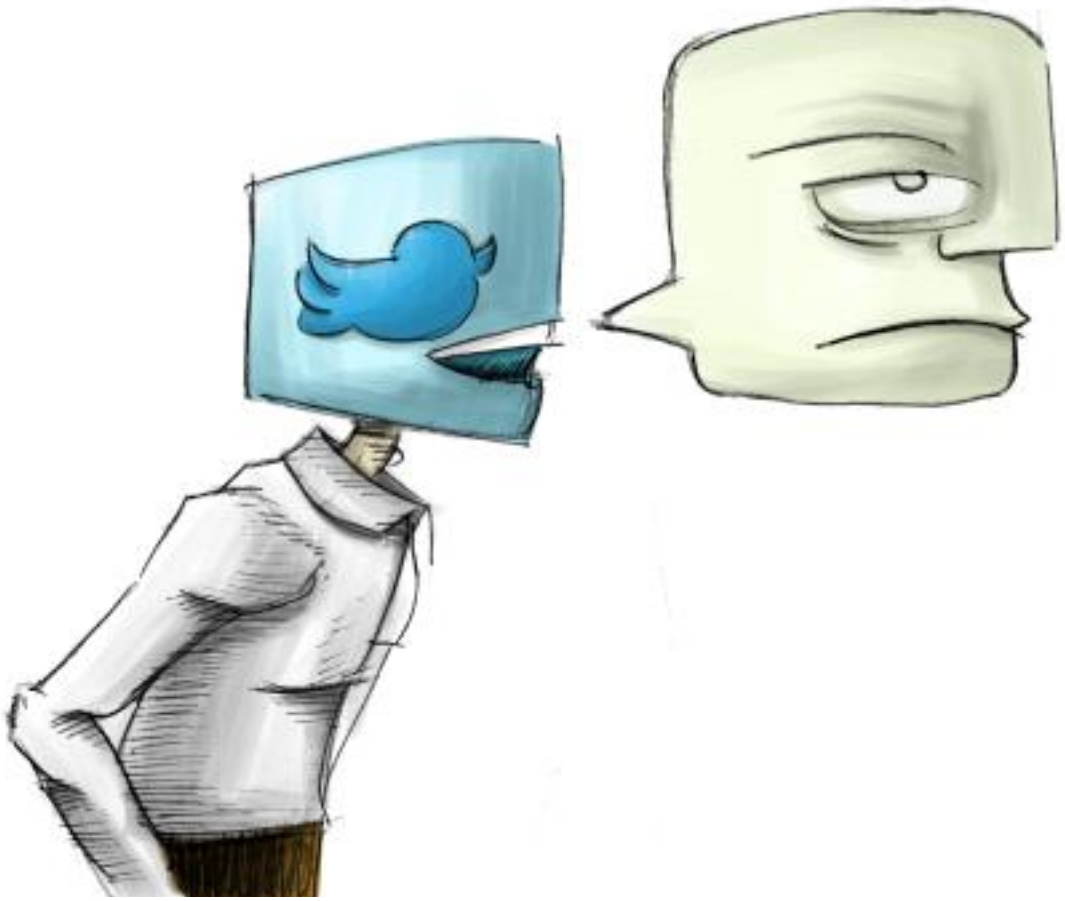
Ing. Oscar Raúl Ortega Pacheco

En Internet creamos una imagen sobre quiénes somos y cómo nos ven los demás. Esta imagen o personalidad se conforma a partir de la información que publicamos en foros, blogs, redes sociales, videos o en los enlaces que compartimos. Además, otras personas pueden contribuir a la construcción de nuestra imagen a través de los comentarios que generan en nuestras páginas o por medio de las imágenes que ellos publican.

En el ámbito personal, la situación es distinta. De acuerdo a un estudio relacionado con la reputación en línea, publicado por Background Check en 2012, el 79% de los reclutadores buscan información en Internet sobre candidatos para conocer sus intereses y actitudes. De ellos, el 86% ha informado a los candidatos que fueron rechazados por la información existente en línea. Por su parte, siete de cada diez usuarios de Internet afirman haber consultado datos sobre un tercero en la red.

Esto representa un gran reto para las empresas, pues cientos, miles y hasta millones de usuarios pueden hablar de manera positiva o negativa acerca de sus productos o servicios, ocasionando cambios en cómo se percibe su marca. Por ello, las organizaciones han desarrollado estrategias para manejar su reputación y así poder dirigir las conversaciones que se refieren a ellos dentro de Internet.

En general, los usuarios no se preocupan de los efectos que tienen sus distintas publicaciones en la web, pues muchas fotografías que normalmente no mostrarían a compañeros de trabajo se publican sin ningún tipo de protección, también es común encontrar datos personales como direcciones, teléfonos o números de tarjetas de crédito. Algunas de las consecuencias de publicar información en la web podrían afectar



nuestra seguridad personal o patrimonial, pero también nuestra identidad y reputación puede dañarse.

Es muy importante que los usuarios tomemos en cuenta que en Internet creamos una imagen sobre quiénes somos y cómo nos ven los demás.
Proteger nuestra identidad en línea requiere del desarrollo de acciones continuas que permitan identificar y resolver la pregunta ¿Qué pueden saber los demás sobre mí a partir de Internet? De esta forma podemos desarrollar las siguientes acciones:

1. Establece tu propia reputación

Toma control acerca de la información que se menciona sobre ti, seguramente tus amigos y contactos podrían publicar fotografías o comentarios y etiquetarlos, es mejor que estés al tanto y que decidas qué información se publica y cuál se rechaza.

2. Identifica qué información se publica en Internet sobre ti

Esta acción puedes llevarla a cabo colocando tu nombre en los diferentes buscadores de Internet. Los resultados pueden mejorar mientras más específicos sean tus criterios de búsqueda. Es importante que tú y tu familia configuren los servicios de redes sociales para recibir notificaciones en el momento en que alguien realice alguna referencia en comentarios y fotos etiquetadas. También puedes considerar algunos servicios en Internet que analizan y te mantienen informado sobre referencias a tu nombre o imágenes en sitios de redes sociales y portales en línea.

3. Evalúa tu reputación en línea

Analiza qué dice en su conjunto toda esta información obtenida sobre ti. Puedes hacer uso de preguntas como ¿La información refleja lo que quiero que otras personas sepan de mí?, ¿hace falta esta información o debería eliminarla?

4. Analiza tus vínculos con otras organizaciones o personas

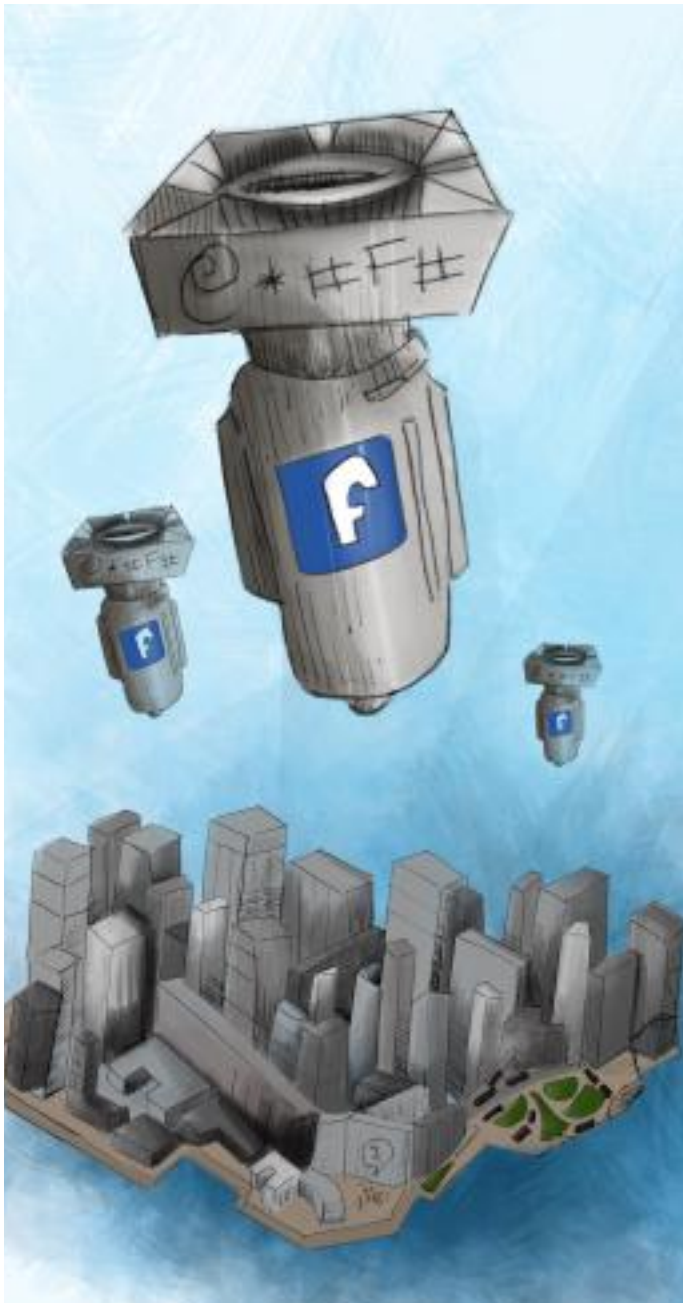
Cuando buscan candidatos, algunos reclutadores toman decisiones en función de las personas o empresas con quienes mantienes contacto en Internet. Considera a contactos profesionales y tu adscripción a grupos de amigos.

5. Publica información con regularidad

Mantener un sitio web, blog o perfil en Internet sin actualizar afecta la percepción que tienen las personas sobre ti, por ello procura actualizar con regularidad, además esto ayudará a mantenerte en los primeros resultados de los motores de búsqueda.

6. Piensa antes de publicar

Antes de publicar cualquier tipo de información, analiza si te sentirás a gusto con el comentario hoy o por ejemplo, en los próximos 10 años. Procura evaluar las consecuencias que podría tener cada comentario e imagen si fuera vista por un familiar, amigo, compañero de trabajo, un reclutador o un profesional en los temas que abordas.



7. Trata a los demás como te gustaría que te trataran a ti

Enviar mensajes negativos a otras personas también puede impactar tu reputación, no solo por malos comentarios, también mantener discusiones en línea podría afectarte al mostrar comportamientos o actitudes conflictivas.

8. Asegura tus cuentas

Utilizar contraseñas seguras y desarrollar buenas prácticas sobre el manejo de tus cuentas previene que usuarios malintencionados accedan fácilmente a ellas para publicar información en tu nombre.

9. Configura opciones de seguridad y privacidad

Busca en los distintos servicios en Internet estas opciones y decide qué imágenes y comentarios deben estar disponibles para las personas que deseas, y no para todos los usuarios de la red.

10. Asesora a tus contactos sobre su reputación

La imagen que reflejan tus amigos y contactos podría afectarte indirectamente, algunas personas podrían asociar sus hábitos, costumbres e ideologías con las tuyas. Por ello, ayuda a tus amigos a que mantengan una buena reputación para que en conjunto, puedan lograr mejores oportunidades.

11. Reporta abusos

Algunos de los usuarios que se conectan a Internet solamente buscan ofender a otras personas, si detectas a algún usuario que lleve a cabo estas prácticas, elimina sus comentarios y busca las opciones de denuncia existentes en las redes sociales y correo electrónico para que sean sancionados.

Una imagen positiva permite a las personas obtener grandes oportunidades en su desarrollo personal y profesional, es una actividad que se lleva a cabo en nuestra vida cotidiana, pero que debe extenderse a las actividades en línea.

El uso de las tecnologías de información y comunicación requiere responsabilidad y respeto en cada una de las actividades que llevemos a cabo. Esto involucra mantenerse informado sobre las distintas tecnologías, sus ventajas y posibles riesgos para que, como usuarios migrantes o nativos digitales, podamos tomar decisiones basadas en el conocimiento obtenido del uso de la tecnología, construyendo una nueva ciudadanía digital que permita a las personas interactuar en ambientes seguros y confiables.

[1] *http://blogs.eset-la.com/laboratorio/2012/08/13/google-reputacion-linea-usuario/*

Normatividad en las organizaciones: Políticas de seguridad de la información- Parte I

Ing. Pablo Antonio Lorenzana Gutiérrez, Ing. Miguel Ángel Mendoza López
Coautores: Ing. Sandra Atonal Jiménez, Ing. Rubén Aquino Luna

En la actualidad, las organizaciones hacen uso de tecnologías de la información para su operación diaria. El logro de sus objetivos se debe en gran medida a su utilización. Sin embargo, existen riesgos inherentes a ellas, es decir, la posibilidad de que una debilidad sea aprovechada por una amenaza y sus consecuencias: divulgación, modificación, pérdida o interrupción de información sensible.

Las herramientas y medios técnicos por sí mismos ya no garantizan un adecuado nivel de seguridad con relación al manejo de la información. En este contexto, las políticas de seguridad surgen como una herramienta para ayudar en el proceso de concientización de los miembros de una organización, sobre la importancia y sensibilidad de la información, además de ofrecer un marco normativo para el uso adecuado de la infraestructura de TI.

De acuerdo con la encuesta The State of Network Security 2012, realizada a más de 180 profesionales de seguridad de la información y TI, la mayoría de los incidentes de seguridad de la información que se producen en las organizaciones son ocasionados por los propios empleados, ya sea por descuido, desconocimiento o intencionalmente, debido a que no existen mecanismos de control que regulen su conducta. En otras palabras, no existen políticas de seguridad de la

información. Si no existe una política, el empleado no dispone de normas, desconoce los límites y responsabilidades asociadas a las actividades que desempeña.

El desarrollo de políticas de seguridad puede verse como una labor complicada debido al bloqueo creativo del responsable durante la redacción y generación de su contenido, generalmente suelen ser víctimas del síndrome de la hoja en blanco. Para evitar esto, es recomendable responder las siguientes interrogantes:

- ¿Quién debe ser la persona responsable de crear las políticas?
- ¿En qué estándar o mejor práctica deben tener base?
- ¿Cuáles son los ámbitos de aplicación?
- ¿Qué estructura debe tener el documento?
- ¿Cómo redactar los enunciados?
- ¿Existen o deben crearse otros documentos que complementen a las políticas?
- ¿Cómo deben difundirse entre los empleados?

La respuesta a cada una de estas preguntas resulta complicada si no se cuenta con los elementos básicos para la elaboración de las políticas. Un elemento esencial es conocer el objetivo y las características que debe poseer un documento como este.

En el ámbito de la seguridad de la información, una política es un documento que describe los requisitos o reglas específicas que deben cumplirse en una organización. Presenta una declaración formal, breve y de alto nivel, que abarca las creencias generales de la organización, metas, objetivos y procedimientos aceptables para un área determinada. Entre otras características:

- Requiere cumplimiento (obligatorio).
- El incumplimiento deriva en una acción disciplinaria.
- Se enfoca en los resultados deseados y no en los medios de ejecución.
- Deben ser concisas y fáciles de entender.
- Deben mantener un balance entre la protección y la productividad.

Las políticas de seguridad de la información proveen un marco para que las mejores prácticas puedan ser seguidas por los empleados, permiten minimizar riesgos y responder a eventos indeseados e inesperados.

También ayudan al personal de la organización a asegurar sus activos, definir la postura de la organización hacia la protección de la información frente a accesos no autorizados, modificación, divulgación o destrucción. De manera específica, las políticas permiten:

- Proteger activos (personas, información, infraestructura y sistemas).
- Definir reglas para la conducta esperada del personal y usuarios.
- Definir roles y responsabilidades del personal.
- Definir y autorizar sanciones en caso de una violación.
- Mitigar riesgos.
- Ayudar en el cumplimiento de leyes, regulaciones y contratos.
- Crear conciencia entre el personal sobre la importancia y protección de los activos, principalmente de la información.

Los beneficios que ofrecen las políticas pueden ser fácilmente descartados si no se definen de manera previa las personas a las cuales están dirigidas (audiencia), lo que determina el sentido de los enunciados escritos. Se pueden tener diversos intereses dentro de la organización, por lo que la audiencia de las políticas puede ser dividida en categorías. Todos los usuarios (lectores) se incluyen en al menos una categoría, por ejemplo:

- Personal administrativo (recursos humanos, contabilidad, etc.).
- Personal técnico (programadores, administradores de sistemas, administradores de red, etc.).
- Usuarios finales.

La audiencia determinará lo que se debe incluir en cada política. Por ejemplo, no siempre se incluirá una descripción del porqué cierta acción es necesaria en una política. Si el lector es responsable de configurar un sistema, es posible que no requiera una explicación del enunciado de la política. Un miembro del personal administrativo conoce los principios y el contexto detrás de esas acciones en un lenguaje no técnico, por lo que tampoco requiere de la explicación. Sin embargo, si el lector es un usuario final, sería útil incorporar una descripción del porqué un control de seguridad es necesario, esto contribuye en el entendimiento y cumplimiento de la política.

La estructura jerárquica también juega un rol importante para el cumplimiento. Es recomendable contar con una política rectora de carácter gerencial, soportada por otro grupo de políticas de carácter técnico, de las cuales pueden derivar guías y/o procedimientos.

• Política rectora

Es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información, establece la importancia de los activos, el qué y porqué una organización planea protegerlos. Debe ser enriquecida con otras políticas dependientes, guías y procedimientos.

• Políticas técnicas

Son más detalladas que la política rectora y definen los elementos necesarios para asegurar los activos. En términos de nivel de detalle, una política técnica establece el qué (a mayor detalle), quién, cuándo y dónde. Describe lo que se debe hacer, pero no la manera de llevarlo a cabo, esto está reservado para las guías y procedimientos. Los temas que pueden ser considerados son:

- Sistemas operativos
- Aplicaciones
- Red
- Administración
- Planes de negocio
- Dispositivos de seguridad
- Dispositivos periféricos
- Dispositivos móviles
- Criptografía
- Seguridad física

• Guías y procedimientos

Proporcionan los pasos a seguir para llevar a cabo los enunciados de las políticas técnicas. Son documentos adjuntos y están escritos en un siguiente nivel de granularidad, ya que describen cómo se deben hacer las cosas. Generalmente, están redactados en un lenguaje técnico avanzado debido a que está dirigido a personal operativo. Por ejemplo, se pueden incluir guías de hardening de sistemas operativos.

Por otro lado, el desarrollo de políticas requiere de la participación de miembros de la organización directamente relacionados con los procesos esenciales de la misma, por lo que es importante contar con un comité o equipo que se encargará de autorizar cambios y actualizaciones de los documentos relacionados (políticas, procedimientos, guías y formatos).

El comité puede estar integrado por personal clave en la operación de la organización, que tenga el conocimiento y dominio de los procesos operativos. Por ejemplo, los jefes de departamento, dueños o custodios de activos, etc. Dentro de sus responsabilidades con relación a las políticas, se debe agregar:

• Aprobar nuevas políticas, iniciativas y actividades.
• Crear, revisar, aprobar y difundir.
• Sancionar violaciones.
• Realizar reuniones periódicas para la revisión, adecuación y cumplimiento.
• Establecer roles y responsabilidades para asegurar que las actividades se realizan en tiempo y forma.

El desarrollo de las políticas inicia con la priorización de los temas que deben abordarse, la identificación del personal al cual van dirigidas y los activos a proteger. Para ello, se pueden realizar las siguientes actividades:

• Seleccionar las áreas que utilicen información que deba ser protegida por alguna ley (nacional, estatal o local).
• Identificar información utilizada para la toma de decisiones críticas dentro de la organización.
• Identificar información crítica para la continuidad de las operaciones.
• Definir la sensibilidad de la información.
• Especificar un esquema de clasificación de información.

Una vez que se han realizado las actividades anteriores, el equipo de desarrollo de políticas debe comenzar la redacción de los documentos y seguir su ciclo de vida, el cual se basa en un proceso de mejora continua.

La identificación de incumplimientos, inconsistencias y la retroalimentación de las partes involucradas permite realizar adecuaciones en los documentos. El ciclo se conforma de cinco fases:

• Escritura

La redacción debe emplear un lenguaje conciso y fácil de comprender, los responsables definen el sentido de la política, evitando el uso de negaciones directas en los enunciados. Por ejemplo, "El usuario debe bloquear su equipo al ausentarse de su lugar de trabajo", es una política que indica lo que está permitido, o "Se prohíbe que el usuario deje un equipo desatendido sin bloquear la sesión", es una política que indica lo que está prohibido. Ambas redacciones son aceptables siguiendo un enfoque permisivo o prohibitivo respectivamente, pero "El usuario no debe dejar su equipo desatendido sin bloquear la sesión" es una redacción de carácter negativo que debe evitarse.

• Revisión

Permite definir el contenido de las políticas de acuerdo a los intereses de la organización, el sentido de la redacción y la funcionalidad de lo descrito en los enunciados, sin afectar las operaciones cotidianas, es decir, mantener un equilibrio entre la funcionalidad y la operatividad.

• Aprobación.

Una vez que hayan sido revisadas y se considere que el contenido es apropiado, las políticas deben ser ratificadas por el comité para su publicación. Se debe incluir la fecha de aprobación.

• Difusión

Una actividad primordial consiste en dar a conocer las políticas y su entrada en vigor, el crear las políticas y no difundirlas resulta un gran esfuerzo desperdiciado. Por tal motivo, el comité debe idear mecanismos para dar a conocerlas entre las audiencias, a través de actividades como la creación de carteles, trípticos, sesiones informativas y otras.

• Actualización

La aplicación de políticas es una actividad permanente y de mejora continua, por lo que pueden realizarse reajustes. La presencia recurrente de la violación de una política, una sugerencia de las partes involucradas, el uso de nueva tecnología o cambios en la estructura organizacional son algunas de las razones por las cuales se actualiza una política.

Con los puntos antes descritos, se pretende dar respuesta a algunas de las interrogantes plasmadas en este artículo, en la segunda entrega se abordará la estructura de los documentos y su alineación a una mejor práctica o estándar.

Los responsables de la creación de políticas deben considerar las operaciones cotidianas, los hábitos y la cultura organizacional, para instar a las audiencias en su aceptación y cumplimiento, basados en el principio de que las políticas no representan restricciones o cargas laborales, sino elementos que permiten proteger los activos al tiempo que madura la operación. De esta manera las organizaciones podrán gozar del beneficio que ofrecen.

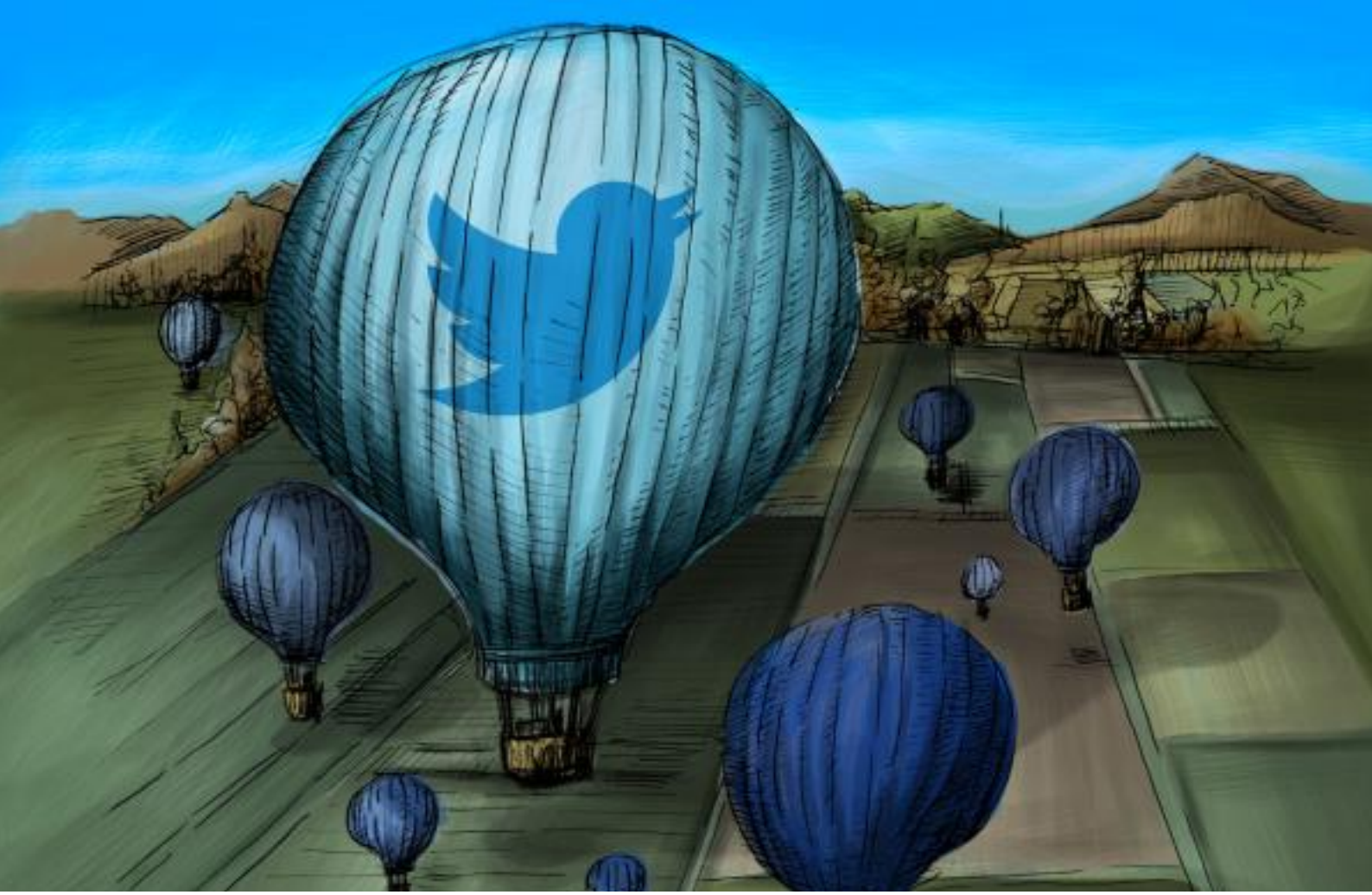
• International Organization for Standardization. ISO/IEC 27001:2005.

• SANS Institute. Information Security Policy - A Development Guide for Large and Small Companies.

• SANS Institute. Security Policy Roadmap - Process for Creating Security Policies.

• SANS Institute. A Short Primer for Developing Security Policies.

• The State of Network Security 2012. AlgoSec Survey Insights.



Lo que el rumor se llevó, crónicas del riesgo reputacional

Ing. Jeffrey Steve Borbón Sanabria

Entiéndase riesgo como el potencial de que una amenaza específica explote las vulnerabilidades de un activo o grupo de activos para ocasionar pérdida y/o daño de los mismos[1].

Lo anterior ilustra al riesgo como aquel personaje molesto con el cual se debe aprender a convivir aunque se desee mantener lo más alejado posible. Conocemos la existencia de riesgos de diferentes aspectos, tales como riesgos financieros, legales o de cumplimiento, operativos, tecnológicos y por supuesto, los de seguridad de la información. Sin embargo, la existencia de un riesgo denominado reputacional o de imagen, plantea la necesidad de entendimiento de otro factor no tomado en cuenta en muchas ocasiones: cuando uno de los riesgos mencionados anteriormente se materializa. A lo largo de este artículo se analizará la forma en que algunas empresas y organizaciones han manejado este riesgo orientado a fallos en seguridad de la información y algunos consejos para entender cómo gestionarlo adecuadamente.

Entendiendo el riesgo reputacional

El riesgo reputacional se comprende como la posibilidad de una opinión o comentarios, que pueden ser positivos o negativos, frente a las actividades, prácticas o situaciones desarrolladas por una compañía y que puede generar un impacto negativo, viéndose reflejado en la reducción de clientes, servicios o caída de ingresos.

El análisis y control de este tipo de riesgo se lleva a cabo comúnmente en instituciones del sector

financiero, dado que una afectación de la imagen o reputación puede verse reflejada directamente en el valor de las acciones o en la desconfianza de inversionistas, quienes podrían no encontrar en la organización la sensación de seguridad suficiente, lo que llevaría a afectaciones en las decisiones de no inversión.

Es posible analizar este tipo de riesgo también como un riesgo consecuencia de otros. El riesgo reputacional aparece usualmente como consecuencia de una explotación de vulnerabilidades o fallos que evidencian riesgos en seguridad de la información y por ende generan de inmediato desconfianza en usuarios y clientes, entre otros. Para contextualizar mejor esta idea, es necesario presentar varios ejemplos de empresas que se han enfrentado al riesgo reputacional asociado a la materialización de riesgos de seguridad de la información o de base tecnológica.

La compañía de videojuegos...

Como primer ejemplo, debemos volver unos años atrás y recordar la ola de ataques que enfrentó la firma Sony y sus filiales a lo largo del mundo durante el año 2011. En dichos ataques, que fueron logrados debido a las relaciones de confianza e infraestructuras similares establecidas entre las filiales de la compañía, se identificó fuga de información relacionada con cuentas de acceso, correos electrónicos y tarjetas de crédito de más de 30 millones de usuarios en todo el mundo.

De acuerdo con análisis realizados por matemáticos de la revista Forbes[4], el costo de los ataques significó a la empresa Sony aproximadamente 24 billones de dólares. Además de todos los costos en pos de mantener a sus clientes y evitar que optaran por cancelar sus cuentas y dejar de usar productos de la compañía, todo esto a partir de numerosos regalos a través de la misma red a sus usuarios, disculpas públicas y múltiples estrategias de mercadeo que hicieron del 2011 un año menos tormentoso de lo que ya era para la firma de videojuegos.

Entidades certificadoras

Ambas compañías pertenecen al mercado de seguridad de la información, ofreciendo servicios de firmado de certificados digitales y cumpliendo un rol como entidades certificadoras dentro de los esquemas de Infraestructura de Llave Pública (PKI).

DigiNotar sufrió un ataque en julio de 2011, en el cual un atacante logró comprometer la infraestructura de la Entidad Certificadora (CA) para generar cientos de certificados digitales falsos de diferentes dominios de alto perfil, tales como Google, Yahoo, Mozilla y Wordpress, entre muchos otros. En este proceso, luego de varias investigaciones realizadas por parte del gobierno alemán y, de haber tomado control de la compañía en el mes de septiembre del mismo año, se determinó que toda la infraestructura había sido comprometida en el ataque. Esto dio lugar a la materialización del riesgo reputacional en torno a la responsabilidad de la compañía en este fallo de seguridad y a la desconfianza de todos sus clientes, lo que llevó a DigiNotar a declararse en bancarrota y cerrar sus puertas[2].

Un segundo caso similar, pero con un final diferente, se registró con la empresa Comodo, la cual logró identificar a tiempo el acceso no autorizado por parte de un reseller a su

plataforma para la realización del firmado de 9 certificados digitales de 7 dominios diferentes. En el mismo ataque lograron comprometer la Autoridad de Registro (RA), parte de la Infraestructura de Llave Pública (PKI) de la compañía. Comodo logró identificar el fallo y solucionarlo 9 días posteriores a la intrusión, registrada el 15 de marzo de 2011[3]. En la actualidad, la compañía aún funciona normalmente. Sin embargo, por más que fue controlada la situación, en el mercado de seguridad de la información (luego del fallo) ha perdido mucho terreno.

Procesos gubernamentales

En el año 2010, durante el proceso de elecciones legislativas llevadas a cabo en Colombia, se presentó un hecho bochornoso relacionado con un ataque contra la infraestructura de la Registraduría Nacional y el Centro Nacional Electoral. Aunque a la fecha de redacción del artículo el tema sigue sin resolverse[5], la ausencia de controles adecuados en un proceso de tal magnitud (que permitió la ejecución de ataques y los fallos en el servicio), pone en tela de juicio la seriedad del proceso de votaciones y, por supuesto, los resultados del mismo. Esto a su vez, significó una afectación al 100% de la imagen del ente estatal encargado de las funciones electorales, además de plantear dudas en la transparencia de los procesos, hecho que puede llegar a generar problemas graves al interior de un Estado.

Como siempre, hay que estar preparados, incluso para lo peor

Analizados los anteriores casos, que esbozan algunas ideas desde diferentes ámbitos de la sociedad, se puede identificar un patrón en común: La aparición del riesgo reputacional como consecuencia de la materialización de riesgos de seguridad de la información. En unos casos, el correcto manejo de la situación posterior a la materialización del riesgo e inicio del efecto bola de nieve de rumores y comentarios negativos, permitió salir adelante a las compañías implicadas. En otros casos, no se dio ese final feliz y, como ocurrió con Diginotar, no hubo tratamiento o solución a la situación.

Sin embargo, se genera la duda fundamental: ¿Se puede estar preparado para una situación así? Aunque no es una respuesta sencilla, sí se pueden implementar controles que ayuden a reducir el posible impacto, a continuación un listado de recomendaciones:

•Identificar cómo puede verse afectada la compañía a través del daño a su reputación, además del impacto a nivel financiero, operativo y legal.

•El riesgo debe medirse, es por ello que una vez identificados y propuestos controles para su gestión, es imperativo establecer criterios de medición, tales como indicadores o métricas que permitan vislumbrar una escala, que a su vez, ofrezca criterios para definir si es necesario aplicar nuevos controles o estrategias más agresivas para evitar la materialización y, por ende, el impacto a las organizaciones. Recordando la premisa que plantea que aquel riesgo que no se mide, no se controla.

•Establecer, ya sea interno o tercerizado, un centro de respuesta a incidentes de seguridad de la información, planteando los posibles escenarios a los que se puede enfrentar la compañía, determinando actividades para el manejo de estas situaciones y definiendo el cómo se monitorearán estos posibles riesgos.

•Debido a que estas situaciones también afectan la continuidad del negocio, es recomendable tener definido un manual de crisis, en caso de materialización de riesgos que puedan tener impacto sobre la imagen y reputación de la compañía. Este documento define quién realizará y cómo se realizará la comunicación con el exterior de la compañía, así como las medidas para lograr controlar la situación y buscar que la organización pueda salir avante lo mejor librada posible.

•Identificar los riesgos a los que se enfrenta la organización. Entender que la seguridad de la información no es un gasto, al contrario, es una inversión que busca evitar realizar gastos asociados a una fuga de información, a una intrusión, un ataque de denegación de servicio, al sabotaje, entre muchas otras opciones, además de tener controles adecuados para ello.

•Aprender de situaciones de este tipo, presentadas con otras empresas o compañías del sector. Esto ayuda a cambiar la mentalidad de que los controles y protecciones se aplican exclusivamente de forma correctiva y no preventiva, este cambio de mentalidad aporta valor al negocio.

Se ha identificado un comportamiento particular de algunas compañías que no publican reporte o información alguna cuando son atacadas y, como resultado, hay alteración de la integridad de datos o se presenta fuga de información. El año anterior, la firma Verisign[6] aceptó que había sido blanco de un ataque unos años atrás, sin haber informado oportunamente. Es obvio en este punto que el silencio busca evitar que se genere este ruido, asociado a rumores y noticias sensacionalistas en tabloides o secciones desinformadoras de tecnología. Sin embargo, es necesario informar oportunamente a los afectados en caso de presentarse un ataque con los alcances antes tratados. En estas situaciones, el silencio puede ser mucho más nocivo de lo que se puede creer.

Para terminar, es necesario hacerse algunas preguntas frente a este delicado tema:

• ¿Estamos realmente preparados para manejar el riesgo reputacional en nuestras organizaciones?
• ¿Entienden las organizaciones y sus mandos administrativos las repercusiones del riesgo reputacional?
• ¿Qué pueden hacer las compañías para lograr un nivel de preparación y madurez para enfrentar el riesgo reputacional?

1] Instituto de Gobierno de TI. COBIT 4.1. "Marco de Trabajo - Objetivos de control – Directrices Generales – Modelos de Madurez", 2007
[2] Análisis del caso Diginotar
http://www.computerworld.com/s/article/9233138/One_year_after_DigiNotar_breach_Fox_IT_details_extent_of_compromise
[3] Reporte del incidente
http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html
[4] http://kotaku.com/5796301/playstation-network-breach-could-carry-a-24-billion-price-tag-in-some-crazy-fantasy-world
[5] http://www.lasillavacia.com/historia/los-cabos-sueltos-sobre-el-ataque-informatico-el-dia-de-elecciones-24670
[6] http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202

Firewall de Aplicación Web (WAF) – Parte I

L.I. Sayonara Díaz Sarahí Méndez

Al desarrollar una aplicación o sitio web, siempre lo hacemos con el fin de que se pueda acceder desde cualquier lugar y que toda persona que desee llegar a ella pueda hacerlo. Es ahí cuando entramos en problemas, ya que no siempre existirá gente que consulte nuestra aplicación web haciendo buen uso, sino que también existirán personas que quieran dañarla o afectar sus servicios. Por esta razón, debemos estar conscientes de que es muy importante no dejar de lado los aspectos de seguridad.

Existen mecanismos de protección a considerar que son importantes al publicar una aplicación web, es recomendable que no los dejes para después, mejor actúa antes de que los problemas vengan a tu aplicación.

Un Firewall de Aplicación Web (WAF), al igual que un firewall convencional, se encarga de proteger tu red. Pero un WAF irá más allá y te ayudará a proteger tus aplicaciones web de ataques que, normalmente, son un dolor de cabeza para los administradores de las aplicaciones o para los dueños de las mismas.

Entender las características de esta tecnología, relativamente nueva, nos ayudará a tomar las medidas que más se adapten a nuestra organización. Empezaremos por mencionar algunas de las características principales de los WAF, es muy importante tomarlas en cuenta antes de llegar al siguiente paso, la implementación de un WAF por ti mismo.

WAF

Para poder entender el funcionamiento y la implementación de un WAF, debemos tener claro qué es un firewall. Es un dispositivo o software que es instalado y configurado en alguna red para filtrar toda la entrada y salida de paquetes. Los firewalls viven en la capa de red y se basan en los permisos o privilegios que se tengan asignados, para poder acceder a lo que los firewall de red estén protegiendo.

A grandes rasgos, un WAF podría definirse como

un dispositivo, plugin del servidor o un conjunto de reglas que filtran y analizan el tráfico web (entre tu servidor web y tu red externa), es decir, los datos que recibimos por parte del usuario y la respuesta que nuestro servidor web arrojará al usuario. Prácticamente se encuentra de intermediario entre tu aplicación y el servidor web que la tiene alojada.

Sin embargo, no ofrecen ninguna clase de protección contra los ataques especializados en explotar vulnerabilidades web. Son muy utilizados en las organizaciones para limitar el acceso de red a sus empleados o para proteger los equipos de ser atacados por virus o software malicioso, entre otros. Así garantizamos que toda la comunicación existente viaja segura entre la red local y la red externa (Internet) conforme a las normas de seguridad que han sido definidas en la instalación.

Los WAF aplican un conjunto de reglas al tráfico HTTP para detectar y bloquear peticiones de tipo CrossSite Scripting (XSS), SQL Injection (SQLi), Remote y Local File Inclusion (LFI), etc.

Muchos de los WAF trabajan comprobando firmas de ataques web conocidos, pero su misión principal es el funcionamiento de ataques como manipulación de parámetros, cabeceras de las peticiones, cookies, XML, Javascript, etc., es decir, se adentran más a los paquetes, teniendo en cuenta el comportamiento del usuario y manteniendo las sesiones de los mismos. Son tan potentes que se encargan de proteger todo tipo de aplicaciones web alojadas en cualquier servidor, no importando tampoco, el lenguaje de programación en el que hayan sido desarrolladas, además actúan antes de que las intrusiones lleguen a la aplicación.

Hemos hablado de que los WAF funcionan con reglas, pero ¿qué son las reglas y cómo funcionan? Las reglas son patrones normalmente escritos como expresiones regulares que se encargan de hacer el filtrado de la información que pasará o no pasará a través de nuestra red.

Una vez que se tienen activadas las reglas, toda la información que pasa a través de nuestro servidor es parseada por estas reglas para que pueda tener acceso. Si en algún momento, la información que está siendo analizada por nuestras reglas encuentra alguna anomalía, se bloquea la petición.

[1]Las 5 fases de procesamiento de las reglas:

1. Cabecera de la solicitud
2. Cuerpo de la solicitud
3. Encabezados de la respuesta
4. Cuerpo de la respuesta
5. Inicio de sesión

Precisamente, estas fases son los puntos clave de partida de la petición que se va a procesar mediante las reglas.
Sintaxis de las reglas:
SecRegla

`VARIABLES OPERADOR [ACCIONES]`

Esta regla hará lo siguiente:

1. Desplegar la colección de variables de la sección **`VARIABLES.`**
2. Aplicar el operador como se especifica en la sección **`OPERADOR`** a las variables desplegadas.
3. Una regla se dispara una vez que se iguala con todas las variables.
4. Al empatar, se ejecutan las acciones por regla o bien se realizan las acciones por defecto.

Básicamente, esa es la estructura que manejan las reglas dentro de un WAF, las cuales son un punto culminante para que el WAF haga el trabajo de bloquear o dejar pasar las peticiones entrantes a tu aplicación web.
Existen otros mecanismos de defensa, tales

como los sistemas de detección de intrusos o los sistemas de prevención de intrusos, los cuales no pueden ser excluidos del reforzamiento de seguridad en las aplicaciones, más bien, deberían manejarse como herramientas complementarias.

Los sistemas de prevención de intrusos son mecanismos físicos o lógicos para la detección de tráfico malicioso con base en firmas o anomalías. La principal diferencia con los sistemas de detección de intrusos es que los sistemas de prevención son dispositivos activos que tienen la característica de actuar bajo demanda, según las alertas detectadas. A esto se le conoce como inline y significa que, a partir de que un evento es detectado, el sistema puede aplicar automáticamente una medida de mitigación.

Los sistemas de prevención de intrusos tienen capacidades de firewall. Por estas características, a este tipo de dispositivos también se les conoce como sistemas de detección y prevención de intrusos. [2]
A diferencia de un WAF, los sistemas de prevención y detección de intrusos (anteriormente mencionados) están basados en firmas conocidas, sin entender el funcionamiento de la aplicación y, por lo tanto, no son capaces de reconocer tendencias, como un número determinado de eventos concretos, altas tasas de falsos positivos (se da cuando un evento se detecta por error como malware o ataque y dicho evento resulta ser legítimo e inofensivo) o simplemente, analizar cómo va navegando el usuario para conectarse a la página web en cuestión.

Otro aspecto interesante a considerar sobre los WAF es que no necesitamos modificar nuestra aplicación web en lo más mínimo, puesto que las configuraciones se hacen directamente en el servidor web que aloja a la aplicación.

Dentro de los WAF existen los llamados parches virtuales, que trabajan en la capa de aplicación y se encargan de analizar las operaciones e interceptar el tráfico de red. Tienen un impacto muy importante ya que, cuando llegan a existir problemas o fallos dentro de una aplicación desarrollada por terceros (el código fuente real de la aplicación de la que estamos haciendo uso

aún NO ha sido modificado para arreglar ciertos fallos que presenta) entran en acción los parches virtuales, haciendo que explotar la vulnerabilidad descubierta no se realice con éxito.

Por ejemplo, considera que tienes montado un sitio web en algún gestor de contenidos (dígase un WordPress, Drupal, Joomla o cualquier otro) y se descubre un "ataque Día Cero". Ese tipo de ataques se realizan contra una aplicación web o un sistema con el objetivo de realizar intrusiones o ejecutar código malicioso debido a que se dan a conocer las vulnerabilidades existentes en un sistema, en un producto, servicio o alguna aplicación. Por lo general, en ese momento dichas vulnerabilidades son desconocidas por los proveedores de servicio, pero puedes estar tranquilo, el WAF se encargará de actualizar automáticamente los parches necesarios sin que el administrador se encargue de este punto. [3]

La gran mayoría de los WAF existentes son capaces de implementar estas actualizaciones de forma automática, ofreciendo protección en un tiempo aceptable, hasta que el proveedor de servicios ponga a disposición de los usuarios un parche disponible.

Ahora que ya conoces qué son los WAF de manera general, queremos mostrarte cómo es que lleva a cabo su funcionamiento y llevarte paso a paso a la implementación de un WAF por tu propia cuenta. En la segunda entrega de esta publicación podrás indagar más sobre estas especificaciones. También preparamos para ti un anexo en donde encontrarás las guías de Instalación y Configuración de un WAF paso por paso, sencillas y fáciles de seguir, para que logres implementar un WAF con éxito.

Es bien sabido que hoy en día es primordial no perder de vista la seguridad sobre nuestras aplicaciones web, si podemos echar mano de implementaciones como estas, mucho mejor.

[1]http://www.modsecurity.org/documentation/ModSecurity2_Rule_Language.pdf

[2]http://revista.seguridad.unam.mx/numero-10/evoluci%C3%B3n-de-los-sistemas-de-detecci%C3%B3n-prevenci%C3%B3n-y-an%C3%A1lisis-de-incidentes

[3]https://www.owasp.org/index.php/Virtual_Patching_Best_Practices

Zarpamos en tecnología

Ing. Jesús Nazareno Torrecillas

El puente de mando tecnológico

Estimados lectores:

Una singladura más dentro de mi etapa profesional comienza a zarpar en estos momentos. El UNAM-CERT me ha invitado a ser su contramaestre de divulgación tecnológica en asuntos de seguridad de la información y temas relacionados con las nuevas tecnologías. Desde estas líneas, deseo servir como punto de referencia a la hora de abordar los proyectos que en materia de Seguridad de la Información tengan en mente llevar a cabo.

Si bien, en muchas publicaciones a nivel internacional, escriben muchos y muy buenos expertos en cualquier materia afín, quiero que mi contribución sea crítica, independiente y diferente; no orientada a recomendar fabricantes, sino tecnologías que ayuden día a día a los profesionales de seguridad de la información.

Si ustedes tienen dudas, recomendaciones, sugerencias o críticas, les ruego me las hagan llegar para que entre todos mejoremos el nivel tecnológico y podamos llegar a la finalización exitosa de proyectos.

Gracias a todos por seguirme.
Ing. Jesús Torrecillas (D.S.E.) Director de Seguridad de Empresa Universidad Pontificia de Comillas.

Limpiando la cubierta

Para que una nave navegue y llegue a buen puerto tras una travesía, lo primero que hay que hacer antes de zarpar, es poner en orden los aparejos, la arboladura, la jarcia, dar el adecuado mantenimiento a las máquinas y limpiar la cubierta de todo aquello que obstaculice el paso a la marinería y que impida la buena ejecución de las maniobras durante el recorrido.

Cada uno de ustedes, mis queridos lectores, son a su entender, expertos en las tecnologías más diversas. Pero en temas de Seguridad de la Información, el camino es bastante arduo y lleno de muchos obstáculos que impiden, en mayor o menor medida, tener un conocimiento amplio de estas tecnologías y una visión objetiva de lo que se debe hacer y de lo que no debemos.

Antes de abordar un proyecto complejo, como el de securizar una compañía, hay que limpiar nuestra mente de obstáculos y reconocer humildemente que el camino será muy árido y duro; para lo cual, es necesario empezar desde el nivel más bajo del proyecto, pero dentro de un entorno no viciado.

Los obstáculos a los que se enfrenta una persona que desea hacer su carrera como experto en seguridad de la información, aunque hay muchos más, los resumo en los siguientes:

Obsolescencia de las tecnologías

Cada pocos meses (incluso cada pocas semanas) las tecnologías evolucionan, se abandonan, se absorben. Nuevos productos, nuevas tendencias, nuevas reglas de juego aparecen en el mercado de las tecnologías de la información. Esto hace que sea necesario que los profesionales estén en un permanente estado de estrés tecnológico ante la avalancha de información que aparece diariamente.

Es sabido que, cuando uno ya está familiarizado con un producto, llega a la conclusión de que ya es obsoleto, lo que genera un cierto grado de frustración profesional.

Tecnologías innovadoras fugaces

Ante un mercado tan agresivo y pujante, muchas compañías de tecnología sacan y sacan productos que muchas veces nacen muertos antes de ver su consolidación en el mercado, pues otros fabricantes se adelantaron a las ideas y fueron más agresivos a la hora de plantear la estrategia de comercialización.

Innumerables certificaciones como experto en seguridad de la información

El nicho de la formación es una línea de negocio que se podría definir como la nueva gallina de los huevos de oro de los fabricantes de software y hardware. Las empresas serias necesitan gente certificada para hacer frente a las normativas como SABOX, ISOs, etc… A su vez, esto hace que empresas muy nuevas tengan legiones de certificadores y expertos certificados, cuyas tarjetas de visita parecen escritas en arameo por la cantidad de siglas que tienen, algunas de ellas antagónicas. Sugiero leer mi artículo publicado hace algunos años y que titulé:
CISSP, CCENT, CISA, CCIE, CCNA, LPT, GIAC, SSCP… ¿Quién da más?, o cómo ser un experto en seguridad informática y no morir en el intento.

Falta de planificación estratégica de las compañías en seguridad de la información

Una parte importante del personal de TI en las empresas, en especial las personas que tienen el poder de decisión en las mismas, duermen tranquilos pensando que, teniendo un buen antivirus, un firewall y un IPS, están protegidos de por vida.

En 2004, Bruce Schneider escribió en su libro Secrets & lies. Digital Security in a networked world (John Wiley & Sons Inc.): Si usted piensa que la tecnología puede resolver sus problemas de seguridad, entonces usted no entiende los problemas de seguridad y tampoco entiende la tecnología.

compleja da mucho juego a que haya un gran número de oportunistas que se crean expertos por estudiarse un manual y, que por su verborrea y labia agresiva, convenzan a la alta dirección de que adquieran tecnologías que luego no van a resolver los problemas inherentes al día a día de (por ejemplo) hacktivismo, ciberterrorismo, espionaje electrónico, pérdida de información estratégica corporativa, etc.

Desconocimiento de la alta dirección de la empresa sobre qué es seguridad de la información

Posiblemente, más del 90% de los expertos certificados y no certificados informáticos en

Tener un departamento de seguridad de la información lleno de expertos, no garantiza que no ocurran eventos y que la información estratégica no se escape por agujeros o brechas de seguridad.

La triste realidad es que, en la mayoría de las empresas en México, se sigue considerando a los expertos en seguridad de la información “pistoleros que ahora usan ratones y teclados”. Esta pobre percepción de una profesión muy

cualquiera de las decenas de certificaciones como experto, no saben vender a la alta dirección la función de seguridad de la información.

Estos expertos en seguridad de la información, cuando se enfrascan en discusiones dialécticas con los que tienen el poder en las organizaciones, acaban frustrados porque no han logrado evangelizar a la alta dirección sobre la problemática actual. Por tanto, la alta dirección no aprueba inversiones estratégicas en estos

conceptos, al no saber para qué los de TI necesitan nuevas tecnologías periódicamente.

El siguiente comentario lo escuché a un junior que intentaba vender a la alta dirección un proyecto de seguridad de la información. Obvio, la alta dirección lo escuchó con complacencia y nunca asignó recursos a alguien que hablaba tan rarito:

"Con el know-how que tenemos, hagamos un tag con los miembros de IT para asignar al team el deployment, según consta en el abstract. De esta forma y atendiendo a mi main-set analizar el rollmap, con el fin de optimizar el workshop para conseguir un roll out efectivo del software para ello tenemos que elegir a un consultant con las capabilities óptimas y de esta forma conseguir un head count preciso a las necesidades."

A la alta dirección hay que hablarle en el lenguaje que ellos entienden: inversión, retorno de inversión, impacto en el negocio, prevención de parada de operación, ejemplos de otras empresas del mismo nivel que tuvieron pérdidas por no haber hecho un plan director de seguridad de la información, etc.

Hasta la próxima travesía,
Ing. Jesús Torrecillas.

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Revista .Seguridad Cultura de prevención para TI
No.16 / enero-febrero 2013 ISSN: 1251478, 1251477