Ciberseguridad: aspectos técnicos

Agustín Solís Pila
Director de Thales Sistemas de Seguridad

Juan Manuel Castro Herranz
Director de Ingeniería de Thales Programas
Miembro del Grupo de Trabajo de Defensa y Seguridad del COIT

En un entorno cada vez más digital, el diseño de sistemas robustos y seguros es una garantía para el correcto avance de casi cualquier industria. Las medidas de seguridad y control pueden ser de índole técnica, organizativa, procedimental y normativa. Agustín Solís Pila y Juan Manuel Castro Herranz se centran en este artículo en las primeras y analizan los principios a tener en cuenta en las distintas fases del ciclo de vida de los sistemas.

La necesidad de ciberseguridad es una realidad operativa:

La mayoría de los sistemas que están en servicio hoy en día fueron diseñados sin seguridad "nativa", y por ello presentan una gran superficie de ataque. El concepto de "seguridad por diseño" es un desarrollo reciente en el ámbito los sistemas de información.

Tanto en el sector público como en el privado, los riesgos y las consecuencias de un ciberataque no se valoran completamente: pérdidas financieras, daño a la reputación y la erosión de la confianza pública en la sociedad de la información.

Los atacantes se han profesionalizado y organizado. Ciertos ataques recientes se asemejan a operaciones militares a gran escala, y han tenido consecuencias económicas y políticas reales con un alto grado de sofisticación técnica.

La prioridad claramente es *detectar las amenazas tan rápidamente como sea posible y mitigar sus peores efectos* como el robo o la alteración de los datos y el daño a los sistemas de información.

Pero también la tecnología y soluciones asociadas a la seguridad evolucionan rápidamente y son riesgos contra los que nos podemos proteger y que pueden ser medidos en términos de negocio.

Internet provee un "puerto seguro" donde los terroristas y delincuentes pueden operar de forma discreta y generar ingresos fuera del alcance de la autoridad de cualquier gobierno.

Hay algunas bases comunes en las formas en que los atacantes operan y los métodos que usan. De hecho, el ciberespacio es probablemente la mejor ilustración de la *importancia del concepto "continuo defensa-seguridad".*

Cuando hablamos de piratas informáticos o terroristas, tendemos a pensar en individuos que trabajan solos y de forma no coordinada. Pero actualmente los ataques son típicamente organizados por organizaciones de atacantes y perpetrados por profesionales que tienen en mente objetivos específicos. Estos ataques se conocen como amenazas persistentes avanzadas (*Advanced Persistent Threats* o APTs), y no hay forma de que una compañía por sí sola pueda protegerse contra estos ataques masivos.

Esta visión de la situación actual puede parecer derrotista, pero los desafíos no son insuperables. Hay arquitecturas, productos y servicios que ya están disponibles para contrarrestar las amenazas, aunque en general no están siendo adecuadamente implementadas a pesar del número creciente de ataques.

Recomendamos la lectura del *whitepaper* titulado *Using Hardware-Enabled Trusted Crypto to Thwart Advanced Threats* (https://www.sans.org/reading-room/whitepapers/analyst/hardware-enabled-trusted-crypto-thwart-advanced-threats-36215), elaborado por el SANS Institute con el patrocinio de Thales, en el que se hace un excelente repaso de la evolución de las medidas de seguridad y se apuntan algunas soluciones de cara al futuro.

Consideración global de la seguridad

Las organizaciones son tan dependientes de los sistemas de información y operacionales (p.e. sistemas de control industrial, del tráfico aéreo, ferroviario, agua, etc.) y de las tecnologías que los sustentan (elementos de interconexión, ordenadores, sistemas operativos, software de aplicaciones de usuario y software de protocolos de comunicaciones, elementos de soporte a la movilidad, teléfonos inteligentes, etc) que deben pasar de una protección convencional pasiva a una ciberdefensa proactiva. Para contrarrestar las APTs es necesario contar con capacidades de detección y respuesta rápida.

Poner barreras (seguridad estática)

La seguridad debe ser una parte integral del proceso de diseño o mejora de un sistema desde el principio (concepto de "seguridad por diseño").

Tres funciones de seguridad deben ser correctamente implementadas: Autenticación (quién), Autorización (qué) y Auditoría (registro fehaciente de actividad).

Empezamos por identificar el nivel de criticidad de los activos y sistemas en términos de disponibilidad, confidencialidad e integridad. Tras un análisis de los riesgos y las amenazas, estableceremos objetivos de seguridad para cada uno de ellos y definiremos las medidas y controles de seguridad para alcanzar esos objetivos. Estas medidas y controles serán de índole técnica, organizativa, procedimental y/o normativa.

En este artículo nos centramos en los aspectos técnicos de la solución, esbozando a continuación una serie de principios a tener en cuenta en las distintas fases del ciclo de vida de los sistemas.

Primer principio: identificar los objetivos de seguridad

Análisis de riesgos riguroso: inventario de bienes esenciales, bienes de soporte y los eventos a evitar. Se formalizan los niveles de riesgo y los objetivos de seguridad, para definir el plan de tratamiento de cada riesgo identificado: aceptar, evitar, reducir o transferir. La reducción de riesgos consiste en la definición de medidas de seguridad, que han de integrarse en las exigencias técnicas y funcionales de los sistemas.

Segundo principio: aislamiento de datos y servicios

Se trata de definir una arquitectura de sistemas mediante la separación de capas, integrando en cada una de ellas las medidas de seguridad adecuadas a su nivel. Cada componente del sistema es responsable de la integridad y confidencialidad de sus datos y no puede acceder directamente a los datos de otro componente. Esto reduce el impacto de un ataque exitoso sobre un componente, pues se impide o al menos dificulta su propagación a los componentes conexos.

Tercer principio: reducir la superficie de ataque

Reducción del número de elementos potencialmente vulnerables y de servicios expuestos, limitando el número de elementos a mantener, la cantidad de parches a aplicar y el riesgo de 0-days (fallos de seguridad no conocidos que pueden ser explotados por un atacante), p.e. la supresión de librerías innecesarias y la personalización del núcleo de Linux.

Cuarto principio: multiplicar las protecciones a diferentes niveles

El atacante debe vencer múltiples barreras para comprometer el sistema. Cada línea de defensa, tiene un rol específico y es autónoma asegurando la resiliencia del sistema aún cuando el ataque venza varias protecciones. Por ejemplo el filtrado de flujos (*firewall* de red o aplicación), menor privilegio de procesos y personas, abastionado de servidores, etc.

Quinto principio: incorporar la seguridad al proceso de desarrollo del software

Utilización de reglas de desarrollo que incorporen el *estado del arte* (p.e. ISO 9126). Los conceptos a emplear son:

- Principios en la arquitectura SW: defensa en profundidad, reducción de la superficie de ataque, aislamiento.
- Factoría software automatizada: trazabilidad de la contribución de los desarrolladores, automatización de la cadena de construcción, control del proceso por el gestor de configuración.
- Aplicar las normas para el desarrollo de aplicaciones securizadas (OWASP, Iniciativa JAVASEC) e incorporar normas de auditabilidad.
- Integrar mecanismos de protección contra inyecciones (XSS, SQL) y de cifrado y firma de datos.

Revisiones de código para verificar su conformidad con las normas de desarrollo.

Sexto principio: integrar soluciones de seguridad de referencia

Usar soluciones certificadas cuando sea necesario para cubrir diferentes dominios funcionales como: autenticación fuerte y control de accesos, firma digital, almacenamiento securizado, etc.

Séptimo principio: integrar la seguridad en el proceso de cualificación

Verificamos la conformidad de la solución con el objetivo de seguridad definido con gestión y trazabilidad de las actuaciones técnicas. Para la validación del sistema realizamos auditorías de arquitectura, configuración y código, pruebas de intrusión, informes de fallos y pruebas de funcionalidad.

Octavo principio: establecer el dossier de homologación

En este dossier recogemos toda la documentación generada en las fases anteriores: análisis de riesgos, medidas detalladas, cuaderno de pruebas funcionales, informes de auditoría, riesgos residuales, y concluimos con la síntesis del nivel de seguridad del sistema en relación con los riesgos identificados.

Mantenimiento de la seguridad

La Ciberseguridad nunca debe ser dada por hecha o conseguida. Debe ser mantenida a lo largo del tiempo y debe evolucionar según los sistemas son actualizados y emergen nuevas vulnerabilidades y amenazas

Detectar y contrarrestar incidentes (seguridad activa)

Hay que ser conscientes de que aunque se obtenga un alto nivel de seguridad de nuestros sistemas por medio de la defensa pasiva mencionada anteriormente, nunca se

podrá alcanzar una protección contra ciertas formas avanzadas de ataque. Un porcentaje de los ataques tendrá éxito y se necesita contar con una adecuada supervisión de seguridad. En este ámbito se usan los Centros de Supervisión de Seguridad (SOC). La tarea primaria de un SOC es la detección y gestión de los incidentes de seguridad, a partir de la información sobre el comportamiento normal de los sistemas bajo supervisión reconocen cualquier actividad sospechosa reportada por las herramientas de detección de intrusiones tales como los *firewalls* y los útiles de análisis de *logs*.

Una vez detectado el incidente se inicia el proceso de valoración, en el que se definirá el incidente y el comportamiento del atacante y se preverán sus consecuencias sobre los activos primarios y los procesos de la organización.

A continuación se deciden las acciones a emprender para contener los daños y restaurar el sistema y, finalmente, se llevan a cabo las acciones decididas.

Una estrategia de seguridad completa y exitosa comprende la gestión de riesgos y la gestión de incidentes.

Anticiparse a los ataques (seguridad proactiva)

Con las redes sociales, la exposición de la información sensible ha crecido. El contenido difundido en Internet, controlado o no por las organizaciones, podría desvelar vulnerabilidades o crear fugas de información sensible.

Con herramientas de inteligencia basadas en procesos de *crawling* e indexación con tecnología *big data*, el análisis de las redes sociales nos puede proveer unos valiosísimos conocimientos sobre la actividad delictiva, lo que nos permitiría anticiparnos a los ataques. Una plataforma de inteligencia permite a los analistas de seguridad lo siguiente:

- Recopilar las fuentes sociales relevantes.
- Analizar y filtrar el contenido de conversaciones sociales, redes sociales y perfiles de "*black hat hackers*".
- Proveer mapeos dinámicos y cuadros de mando que ayuden a los analistas.
- Enviar informes de alertas y ayudar a los operadores a anticipar, e incluso, desbaratar ataques.

Finalmente, creemos imprescindible mencionar que por muy bien que se gestione la seguridad, los usuarios juegan un rol vital. Deben ser permanentemente concienciados, entrenados e informados con el fin de elevar el nivel de madurez de la organización en términos de seguridad de la información.

Es también importante que las organizaciones se mantengan informadas de los ataques que se producen y el estado de seguridad de sus sistemas. Los CERTs (Computer Emergency Response Teams) proveen este tipo de información.

Conclusión

La ciberseguridad es una meta alcanzable en nuestra sociedad de la información, permitiendo a las organizaciones operar, comerciar y expandirse en el mundo digital actual. Para ello es necesaria la correcta aplicación de normativa en el desarrollo de servicios y productos pues la base tecnológica de la amenaza es la misma que la de la construcción de los sistemas, de forma que se van a explotar las vulnerabilidades y errores cometidos en su desarrollo o explotación. Los productos y servicios de confianza de última generación son de vital importancia, porque, según informes de diversos organismos nacionales e internacionales, el 80% de nuestra economía depende de tecnologías digitales y, por tanto, de la seguridad de los sistemas de información y operacionales.

Cybersecurity: Technical Aspects

In an ever-more digital environment, the design of robust and secure systems is the only guarantee for the smooth progress of almost any industry. Security and control measures can be of a technical, organizational, procedural and/or regulatory nature. Agustín Solis and Juan Manuel Castro Pila Herranz focus in this article on the first of these, and analyze the principles to be considered over the course of the phases in system life cycles.