



¿QUÉ PREOCUPA?

SOBRE BASES SEGURAS

En los últimos años se han producido cambios drásticos en las condiciones de trabajo de todos los que se dedican a la Seguridad de Sistemas, motivados entre otros por los siguientes factores:

1— La enorme extensión de las tecnologías de la información, que en la actualidad son ya parte fundamental de nuestra vida profesional y personal.

2— Apertura y comunicación (Internet, teletrabajo)

3— Evolución hacia entornos abiertos, estándares y la utilización de tecnologías asequibles al usuario doméstico.

... Y todo ello obediendo a los importantes requerimientos de expansión, cambio y competitividad en los negocios a los que se da soporte.

A las indiscutibles ventajas que aporta a los usuarios la infraestructura técnica y las aplicaciones que se han puesto a su disposición, se han

aplicaciones); los responsables de Seguridad de Sistemas en la actualidad deben actuar como el entrenador en un equipo de fútbol, intentando que cada jugador (responsables técnicos y de desarrollo, responsables usuarios, etc..) tenga claros los criterios básicos a respetar por todos y la función a realizar por cada uno, de forma que el equipo, funcionando de manera coordinada, esté en disposición de aplicar y hacer efectivas tácticas o herramientas de ataque o defensa.

Conceptos básicos

Transformar la actividad en torno a la seguridad en algo metódico y pro-activo; para ello hay que actuar en las primeras fases del ciclo de vida de cualquier sistema informático:

— Estableciendo criterios claros de seguridad para el diseño, desarrollo e implantación de las aplicaciones y de las infraestructuras técnicas.

otros, los responsables finales de lo que se haga con un sistema informático y por lo tanto con los datos que maneja.

— Lógicamente, los responsables de Seguridad de Sistemas no pueden mantenerse al margen; deben propiciar la elaboración e implantación de normativas, procedimientos y herramientas que faciliten el trabajo a los distintos agentes que intervienen en el proceso de gestión/administración de la seguridad, y que garanticen que se realiza según los criterios establecidos. En este sentido es muy importante que exista una política clara, y que queden bien definidas las responsabilidades, sobre la acreditación de nuevos usuarios y la asignación de códigos de acceso, sobre la administración funcional (asignación de perfiles de acceso) y sobre la administración técnica.

— Los responsables de Seguridad de Sistemas deberán, además, establecer los controles necesarios para asegurar que la explotación de los sistemas informáticos se realiza de una forma estable y segura.

Sobre esta base podremos intentar, con ciertas garantías de éxito, aplicar procedimientos y herramientas de seguridad para conseguir una protección efectiva, hacer de la seguridad algo objetivable y por lo tanto gestionable, evitando el riesgo de convertirnos en bomberos o, lo que es peor, en chivos expiatorios de situaciones de las que nadie se siente responsable, y posiblemente nadie en especial lo sea.

Una vez que hemos llegado a esta conclusión, tomamos contacto con la dificultad típica de las disciplinas horizontales para materializar sus líneas de acción; debemos solicitar a todos los agentes participantes en el ciclo de vida de un sistema informático que dediquen parte de su presupuesto a tareas sin una visibilidad clara en el producto para usuarios y/o clientes, sobre todo en años de ajuste presupuestario, como son últimamente todos.

Posiblemente sea un problema de madurez, y podamos aprender bastante en este sentido de otras disciplinas como la Calidad, que han sabido encontrar su sitio en nuestra metodología de trabajo, partiendo incluso de posiciones de más difícil justificación que la nuestra.

En cualquier caso, independientemente de la dificultad, creo que esta es una línea de trabajo fundamental, y que de nuestra habilidad para plantearla y afrontarla adecuadamente, sobre todo hacia el futuro, depende gran parte del éxito de nuestro trabajo. ■

Hay que hacer de la seguridad algo objetivable y por lo tanto gestionable, evitando el riesgo de convertirnos en bomberos o, lo que es peor, en chivos expiatorios

añadido un conjunto de nuevas e inquietantes amenazas (virus, intrusismo, *spam*, etc.) de las que se es cada vez más consciente, y para cuyo tratamiento aparecen constantemente en el mercado nuevas herramientas.

Esta situación plantea un importante reto para los responsables de Seguridad de Sistemas, que deben establecer procesos y procedimientos capaces de detectar los problemas con rapidez, buscar las salvaguardas más adecuadas y aplicarlas en el mínimo tiempo posible... En muchos casos, misión imposible. A pesar de que los presupuestos de seguridad aumentan, al final, la sensación puede ser la de no conseguir una mejora importante, y en cualquier caso efímera, hasta el punto de definir la Seguridad como gestión del riesgo, conscientes de la gran dificultad, en algunos casos, de conseguir un marco claro de seguridad.

Pero, ¿dónde se encuentra el principal factor de riesgo? En mi opinión el nivel de riesgo que se soporta puede ser debido tanto a las amenazas existentes, como al hecho de que se produzcan sobre unos entornos (infraestructura y aplicaciones) que, por su acelerado ritmo de implantación y cambio, no han seguido unos criterios adecuados en su diseño, desarrollo e implantación.

Y, ¿cuál es la línea de actuación más adecuada en este sentido? La única forma de conseguir una adecuada efectividad con los controles que establezcamos pasa por trabajar en el afianzamiento de los conceptos básicos que pongan orden en nuestra arquitectura (infraestructura y

Una vez en explotación, nos veremos obligados a actuar de forma reactiva, pero que hay que evitar que sea en lo fundamental, en lo básico.

— La infraestructura técnica debe contemplarse como un conjunto a proteger, y esta estrategia de protección debe constituir la envolvente con la que obligatoriamente deben ser coherentes las de cada uno de sus componentes.

— En el desarrollo interno de aplicaciones, la utilización de componentes comunes de seguridad estrechamente controlados para la autenticación y control de accesos, además de una mejora de la seguridad, producirá claros ahorros en tiempo de desarrollo.

— Las aplicaciones adquiridas deben respetar los estándares de mercado e integrarse adecuadamente en nuestra arquitectura de seguridad. La seguridad debe ser también un criterio importante en su proceso de selección

— Los datos son el corazón de nuestro negocio; es imprescindible exigir métodos seguros de acceso a las bases de datos.

En resumen, la seguridad debe formar parte fundamental de la metodología de diseño, desarrollo e implantación de sistemas e infraestructuras.

Otro de los aspectos fundamentales consiste en la fijación y difusión clara de roles, obligaciones y responsabilidades en el tratamiento de la información.

— Los sistemas son un instrumento diseñado siguiendo las instrucciones de los responsables funcionales y utilizados por los usuarios según los perfiles que aquellos les asignan. Ellos son, y no



> Manuel Martínez García
Seguridad de Sistemas
Tecnología de Sistemas

UNIÓN FENOSA, S.A.