



¿QUÉ
PREOCUPA?

DESDE LA TRINCHERA

Ser invitado a escribir en esta sección de SIC y poder exponer a colegas de seguridad mis pensamientos sobre el tema, supone un gran honor y reto. Por ello mi primera idea fue hablar muy formalmente de planteamientos para una creación de la gestión de seguridad en la empresa, de planificación de actividades y desarrollos necesarios, de la visión empresarial que debe guiar la existencia del departamento y, en fin, toda una serie de arduos conceptos que deben tenerse en cuenta para esa actividad como otra área más de la empresa y sus riesgos. Pero creo que ya destacados autores muy cualificados han escrito aquí sesudos estudios sobre ello, y yo humildemente poco podría aportar diferente.

La seguridad es la única disciplina informática de la que todos se atreven a opinar. Pocos juzgarán el enrutado, los sistemas de *backup* o los *teraflops*, pero cuando estés ante un problema, no faltarán tres o cuatro benditos que te pregunten "¿tenéis antivirus?"

Ahora bien, después de los grandes planteamientos, estrategias y decisiones siempre viene la realidad diaria; es decir, que estás sólo en el frente del día a día, enfrentándote a *hackers*, virus, vulnerabilidades, técnicos celosos, usuarios listillos, usuarios quejosos, estafadores, enormes *logs* y escasos presupuestos.

Así que en "¿Qué preocupa?" he considerado más conveniente –y ligero de leer– resumir algunas preocupaciones, reflexiones personales, vivencias y trucos que colegas míos y yo, como soldados veteranos, nos hemos confesado o compartido en la soledad de nuestras trincheras con la esperanza de que sean consejos que puedan servir a cualquier nuevo administrador de seguridad.

Sobre estrategia

Ten siempre presente que la seguridad es sólo poder responder a cuatro preguntas:

1. ¿Quién existe en mis sistemas? Si no sabes identificar de golpe a cada quien que anda en ellos, mal sabrás distinguir quién es intruso. Utiliza identificadores de usuario únicos, huye de los genéricos, crea una administración sólida y enlaza inexorablemente con RR.HH.

2. ¿Cuáles son los recursos a proteger? Si no conoces el inventario mal sa-

brás qué proteger. Haz tus estudios de riesgo, pero si te desbordan, adopta uno simple: protege mejor todos los datos de explotación y cierra cualquier camino que conduzca a ellos.

3. Dado un usuario, ¿a qué puede acceder? Debes estar en disposición de responderlo para poder cortarles totalmente el acceso cuando sea urgente.

4. Dado un recurso, ¿quién puede llegar hasta él y por dónde? Si puedes responder esto para cualquier recurso, sabrás qué camino debes proteger y tendrás mucho ganado.

Sé corporativo; no puedes luchar sólo. Confía a tus colegas de Sistemas los problemas que ves, propón soluciones y acciones conjuntas. Persigue mutuamente con

ellos parches de soft y hard, ya que tú no puedes perturbar el funcionamiento por muchos arreglos que estés tentado de exigir. Reclama incesantemente la colaboración de Dirección.

Comunica siempre por escrito las necesidades que veas de emprender acciones de defensa o prevención; en seguridad es importante poder demostrar que no hubo indolencia. Y documenta, porque te lo agradecerás tú mismo cuando haya prisa.

Sé ecuaníme en los costes. La seguridad cuesta y sirve, pero comprende que es más fácil vender un "nuevo pintado bonito del coche" antes que un "cinturón de seguridad de tres puntos de anclaje" cuyas ventajas sólo entienden los expertos y que quedará obsoleto.

Pelea a fondo para que la seguridad se tenga en cuenta en las aplicaciones desde la fase de diseño. Pon en tela de juicio los "magníficos" paquetes comerciales que para funcionar en tu empresa requieren que desarmes tres o cuatro reglas de seguridad. Protesta, paraliza su despliegue o sugiere alternativas, pero crea la cultura de que las aplicaciones deben ser seguras por diseño.

Sobre armas

No utilices excesivas armas. Te bastarán los cortafuegos, IDS, antivirus, herramien-

tas de gestión de usuarios, detectores de vulnerabilidades y poco más. Pero ten en cuenta que, aparte del presupuesto limitado, todas ellas requieren expertos y examinar luego sus *logs* e incidentes, y el día a día no te dará mucho tiempo. Adezca con políticas y auditorías.

Utiliza ampliamente tu sexto sentido. Hay detalles irrelevantes que te pueden poner en la pista de un gran problema: una coma que aparece en un *log* donde antes no estaba, un usuario que cuenta como su pantalla repentinamente se ha puesto verde, un mensaje de error, un pequeño apunte inesperado anoche a las tres de la madrugada... Tira del hilo.

Sobre personas

Cuida a tu personal. Gestionar la seguridad requiere prisa y desgasta mucho, y los maliciosos ya no tienen horario, con lo que las personas acaban acusándolo.

Presta atención a las conversaciones triviales. Probablemente cualquier programador joven recién llegado sabrá mucho más que tú sobre Java, html, *exploits*, *cracks*, *J2C*, *scripts* y similares, y es divertido alardear de saltarnos normas. Habla con ellos y aprende.

Somos humanos y descuidamos lo obvio: repasa que los administradores no tengan contraseñas en blanco, que se hayan cambiado las de defecto, que los datos se sirvan cifrados, que haya registro de actividad (aunque consuma disco y cpu)...

Un par de consejos

Ten paciencia. La seguridad es la única disciplina informática de la que todos se atreven a opinar. Pocos juzgarán el enrutado, los sistemas de *backup* o los *teraflops*, pero cuando estés ante un problema, no faltarán tres o cuatro benditos que te pregunten "¿tenéis antivirus?".

Finalmente, nunca estés seguro de estar seguro. A todo hay quien gana, y los *hackers*, creadores de virus, vulnerabilidades y demás malicias, tienen más tiempo que tú para intentar de todo. No te confíes; ¡esto es la guerra! ■



> José Díaz Lifante
Gerente de Seguridad Lógica

BANESTO