Seguridad de la información en la empresa

Los 10 mandamientos para proteger sus datos

Partiendo del concepto de que un proyecto de seguridad no empieza y termina, sino que es un proceso continuo, ofrecemos una serie de pautas a tener en cuenta a la hora de proteger la información y los datos sensibles que una empresa no desea que sean vulnerados.

Osvaldo Callegari
Analista de sistemas - *ocalle@ar.inter.net*

La resonancia alcanzada por el caso Wikileaks y las recientes intrusiones a bases de datos de prestigiosas empresas como Sony, ubicaron al tema de la fuga de información entre los más discutidos y controversiales de la agenda de medios. Si bien no se trata de una problemática nueva, su creciente difusión permitió a las empresas tomar mayor conciencia sobre el valor de su información y la importancia de la privacidad y confidencialidad de la misma.

"La existencia misma del caso Wikileaks determinó un antes y un después en lo que a fuga de información se refiere. No es que antes no ocurriera, sino que -en muchas ocasiones- las fugas no se hacen públicas, con el fin de salvaguardar la imagen de las empresas e instituciones. Además, el incidente permitió entender que si este tipo de incidentes puede sucederle a organizaciones tan grandes y preparadas, podría ocurrirle también a empresas y organizaciones más pequeñas", aseguró el Gerente de Educación & Servicios de ESET Latinoamérica, Sebastián Bortnik.

Es importante comprender a la seguridad como un proceso, dado que la protección de la información no es un proyecto con inicio y final, sino un proceso continuo.

PROTECCIÓN DE LA INFORMACIÓN

La protección en la empresa tiene una característica muy particular: no está en juego la privacidad del usuario o la pérdida de fotos personales, sino que un incidente de seguridad puede perjudicar directamente al negocio, especialmente en términos económicos. Por eso, así como en el entorno hogareño deben combinarse las tecnologías con la educación del usuario, en el entorno de la empresa es necesario agregar un nuevo componente: la gestión de la seguridad.

La implementación aislada de controles de seguridad no termina de ser un enfoque eficiente para la protección de la información de las compañías. En ese sentido, debe entenderse a la protección de los datos como un proceso continuo.

Con el primordial objetivo de contribuir con la educación e información de las empresas, para alcanzar una mejor política de seguridad de la información, los especialistas de ESET han elaborado los 10 mandamientos de la seguridad corporativa, entendidos como los principios básicos que deben regir la protección de la información en las empresas

1. DEFINIRÁS UNA POLÍTICA DE SEGURIDAD

Es el documento que rige toda la seguridad de la información en la compañía. No debe ser muy extensa (ningún empleado podrá comprometerse con un documento de 50 páginas), debe ser realista y es recomendable que sean entregadas a los empleados por los altos cargos o el departamento de Recursos Humanos, en lugar del soporte técnico de IT, para darles valor.

2. UTILIZARÁS TECNOLOGÍAS DE SEGURIDAD

Son la base de la seguridad de la información en la empresa. Una red que no cuente con protección antivirus, un firewall o una herramienta antispam estará demasiado expuesta como para cubrir la protección con otros controles. Según lo presentado en el ESET Security Report Latinoamérica, el 46% de las empresas de la región se infectó con malware en el último año.

3. EDUCARÁS A TUS USUARIOS

Es necesaria la aclaración: educarás a todos tus usuarios. Los usuarios técnicos o del departamento de IT suelen ser omitidos en este tipo de iniciativas, como si estuviera comprobado que están menos expuestos a las amenazas informáticas. Según las estadísticas de ThreatSense.Net, el 45% de las amenazas detectadas en la región utiliza Ingeniería Social, por lo que atentan contra el desconocimiento del usuario para infectarlo.

4. CONTROLARÁS EL ACCESO FÍSICO A LA INFORMACIÓN

La seguridad de la información no es un problema que deba abarcar sólo la información "virtual", sino también los soportes físicos donde ésta es almacenada. También deben ser considerados los datos impresos, como por ejemplo el acceso físico a oficinas con información confidencial (el gerente, el contador, entre otros.); o el acceso a las impresoras (¿alguien podría tomar "accidentalmente" información confidencial?).

5. ACTUALIZARÁS TU SOFTWARE

Las vulnerabilidades de software son la puerta de acceso a muchos ataques que atentan contra la organización. Según el informe sobre el estado del malware en Latinoamérica, el 41% de los dispositivos USB está infectado y el 17% del malware utiliza explotación de vulnerabilidades.

Mantener tanto el sistema operativo, como el resto de las aplicaciones, con los últimos parches de seguridad, es una medida de seguridad indispensable.

6. NO UTILIZARÁS A *IT* COMO TU EQUIPO DE SEGURIDAD INFORMÁTICA

Es uno de los errores más frecuentes en los que se suele ocurrir, omitiendo, además, la importancia de entender que la seguridad, no es un problema meramente tecnológico.

Además, es importante que exista un área cuyo único objetivo sea la seguridad de la información, y ésta no pueda ser relegada por otros objetivos asociados a la usabilidad.

La vulnerabilidad del software es el acceso a muchos ataques contra una empresa. En Latinoamérica, el 41% de los USB está infectado y el 17% del malware utiliza la explotación de vulnerabilidades.

7. NO USARÁS USUARIOS ADMINISTRATIVOS

De esta forma, una intrusión al sistema estará limitada en cuanto al daño pueda causar en el mismo. Una vez más, vale destacar la importancia de aplicar este control a toda la empresa: los integrantes del departamento de IT o la alta gerencia, también deben utilizar permisos limitados en el uso diario de la computadora.

8. NO INVERTIRÁS DINERO EN SEGURIDAD, ¡SIN PENSAR!

La seguridad debe ser concebida para proteger la información y, por ende, el negocio. Hacer inversiones en seguridad, sin medir el valor de la información que se está protegiendo, y la probabilidad de pérdidas por incidentes; puede derivar en dinero mal invertido, o básicamente en dinero perdido.

9. NO TERMINARÁS UN PROYECTO EN SEGURIDAD

Sé que parece extraño, pero no lo es, porque tampoco empezarás un proyecto. La seguridad debe ser concebida como un proceso continuo, que no termina. Es cierto que pequeñas implementaciones de los controles pueden necesitar de proyectos, pero la protección general de la información no puede ser pensada como un proyecto, sino como una etapa de mejora continua, como una necesidad permanente del negocio.

10. NO SUBESTIMARÁS A LA SEGURIDAD DE LA INFORMACIÓN

Finalmente, entender el valor que asigna al negocio tener la información protegida, es nuestro último y quizás más importante mandamiento. Pensar que un control no debe implementarse, porque "no creo que esto me ocurra", es uno de los peores errores que un ejecutivo puede cometer y, en caso de que ocurra, serán muchos los que deban arrepentirse: muchas empresas, especialmente las pequeñas y medianas, no pueden recuperarse de un incidente de gravedad contra la seguridad de la información. ■