UNIVERSIA
BusinessReview

La seguridad camina hacia la madurez

Moisés Navarro[1]
Responsable de Consultoría Tecnológica
IBM España
m.navarro@es.ibm.com

Security evolves towards maturity

INTRODUCCIÓN

El concepto de seguridad tecnológica ha ido evolucionando. En los años 80, los esfuerzos de las empresas y proveedores se centraban en blindar sistemas, que frecuentemente, estaban aislados entre sí. En los 90, la generalización del uso de Internet en el mundo de los negocios planteó nuevos riesgos que alertaron a las empresas en la necesidad de tratar este asunto. Comenzaron a surgir tópicos e incluso modas en la seguridad, que llevaban a abordar acciones que, a menudo, no estaban enmarcadas dentro de una estrategia definida. En la década de 2000, las empresas empezaron a ver que era necesario unir seguridad con el negocio ya que son dos conceptos que no se pueden separar. A pesar de los mensajes, que a menudo son alarmistas, en este momento podemos asegurar que

RESUMEN DEL ARTÍCULO

En los últimos años hemos visto cómo las empresas españolas han iniciado un proceso hacia la madurez en su aproximación al área de seguridad. Sin embargo, todavía queda camino por recorrer. Hay muchas empresas que consideran que la seguridad es una cuestión que se soluciona con la implantación de los productos tecnológicos más sofisticados del mercado. No obstante, la seguridad no es una cuestión de producto, sino de estrategia. En este artículo, Moisés Navarro, de IBM, expone las claves para orientar a las empresas a la hora de abordar la seguridad.

EXECUTIVE SUMMARY

In the last years we have seen how Spanish companies have initiated a process towards maturity in their approach to the security. However there is still a long way to walk. There are many companies that consider that security is solved with the implementation of cutting edge technology products. However to be successful, security should be considered as a strategy, not just as a product issue. In this article, Moisés Navarro from IBM, exposes the key issues that will help companies approaching security.

CODIGOS JEL:
M190

las empresas españolas han iniciado un proceso hacia la madurez en el área de seguridad. Sin embargo, todavía queda camino por recorrer.

SITUACIÓN ACTUAL

En el último año, hemos observado una evolución en los ataques a los sistemas informáticos de las empresas. A diferencia de años anteriores, en los que los ataques eran generales y tenían como objetivo interferir en el rendimiento de los sistemas informáticos, en 2005 detectamos que, cada vez más, el objetivo de los hackers era sustraer datos críticos (identificaciones, dinero, propiedad intelectual, etc.) de las organizaciones con el fin principal de lucrarse, y, en un segundo lugar perjudicar la imagen de marca de una empresa o de sus clientes. Se trata de ataques específicos dirigidos a empresas, instituciones y organizaciones públicas.

Los métodos tradicionales de seguridad, que generalmente eran reactivos, ya no son suficientes para combatir estos ataques de carácter organizado y preparados específicamente para su destinatario.

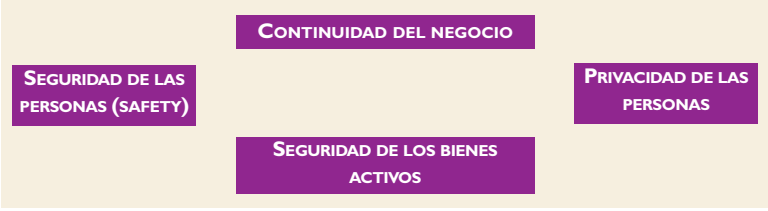
Hay muchas empresas que consideran que la seguridad es una cuestión que se soluciona con la implantación de los productos tecnológicos más sofisticados

Junto con esta evolución del perfil del "hacker", vemos también que cada vez más la tecnología está presente en todos los procesos de negocio de las empresas. Una interrupción en el funcionamiento de los sistemas informáticos de una empresa (ya sea por la entrada de virus, por desastres naturales, o una interrupción del suministro eléctrico, etc.) tiene, generalmente, una repercusión directa en el negocio.

Además, muchas empresas están utilizando las tecnologías como vía para comercializar sus productos y servicios (Internet, mensajes de texto a través de teléfonos móviles, conexiones inalámbricas, etc.). Para estas empresas la confianza se ha convertido en uno de sus objetivos claros, puesto que de ella depende el rendimiento de su negocio.

Por lo tanto, la seguridad es un aspecto que cada vez cobra más relevancia en el mundo de los negocios. De hecho, según datos de un informe elaborado por IBM, el 35% de los encuestados españoles percibe el ciberdelito como una amenaza mayor para sus negocios que la que constituyen los delitos físicos.

A menudo las empresas se sienten seguras implantando productos informáticos sofisticados, pero se olvidan de otros aspectos que son



PALABRAS CLAVE
Seguridad, madurez, estrategia, continuidad del negocio, privacidad, estándares, tecnología

KEY WORDS
security, safety, strategy, business continuity, privacy, standards, technology

básicos. De qué nos sirve tener la caja fuerte más robusta del mercado, si la combinación es tan compleja que al final sus usuarios acaban dejando la puerta abierta.

La seguridad no debe ser percibida como una cuestión meramente tecnológica porque la implantación de soluciones informáticas no garantiza por sí sola la seguridad. La seguridad se ha de abordar como una estrategia con una visión global que comienza haciendo un análisis de los procesos de negocio para determinar, posteriormente, qué mecanismos de seguridad se deben desplegar para dar apoyo a la estrategia que se ha definido anteriormente. Asimismo, no hay que olvidar aspectos tan relevantes como o el factor humano, establecer políticas de seguridad, métricas de la eficacia de estas medidas, análisis de riesgos, etc.

VISIÓN GLOBAL

En primer lugar, para abordar adecuadamente la seguridad, es conveniente determinar qué áreas cubre el concepto de seguridad, teniendo una visión global de este concepto. Así evitaremos dejar de lado áreas de actuación claves y relevantes para el negocio.

IBM considera que el área de seguridad debe de tener una estructura específica que cubre los siguientes planos:

• **Continuidad del negocio:** se trata de asegurar que las actividades de una empresa estén siempre en funcionamiento y que no sufran interrupciones. En cualquier momento, la instalación informática de una empresa puede quedar total o parcialmente inoperativa como consecuencia de un siniestro fortuito (incendios, ataques terroristas, virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, piratas informáticos, errores humanos, etc.). Es importante que la empresa disponga de un plan (de contingencia) que contemple todos los aspectos necesarios para que, en caso de desastre, la empresa pueda recuperar sus datos y restablecer sus operaciones inmediatamente.

• **Seguridad de los bienes y activos (físicos y lógicos):** engloba seguridad de todos los bienes y activos de la empresa, desde la infraestructura tecnológica, hasta los propios datos que posea esa empresa.

• **Privacidad de las personas:** trata todo lo relacionado con garantizar la privacidad de la información personal y el uso que las organizaciones hacen de la información que obtienen de sus clientes, de los ciudadanos o de sus empleados. La privacidad ha adquirido una relevancia muy importante y en España viene regulada por la Ley Orgánica para la Protección de Datos de Carácter Personal y los Reales Decretos que la desarrollan.

• **Seguridad de las personas:** se trata de prevenir y minimizar daños físicos que puedan sufrir las personas como consecuencia de una ruptura en los mecanismos de seguridad de la empresa. Es decir proteger a los empleados en su lugar de trabajo, así como a los clientes e incluso a los ciudadanos.

ESTRATEGIA

Aunque la seguridad esté en la agenda de los directivos españoles, en muchas ocasiones el discurso de seguridad se centra en cuestiones puramente técnicas, muy ligadas a la tecnología y a los productos. Se habla mucho sobre cortafuegos, antivirus, redes privadas virtuales (VPN's), longitud de las contraseñas, longitud de las claves de cifrado, etc. y poco sobre políticas de seguridad, métricas de la eficacia de estas medidas, análisis de riesgos, gestión, etc.

Es decir, a veces las empresas se centran demasiado en las capacidades técnicas de la solución implantada (por ejemplo, un cortafuegos), o en las características que tienen que tener las contraseñas, olvidando aspectos tan relevantes como, por ejemplo, mantener actualizado dicho cortafuegos o el factor humano, que hace que si la contraseña es demasiado compleja, algún usuario decida mantenerla anotada en un lugar visible y cercano a su ordenador.

Es importante trabajar la seguridad como un proceso, estructurado, apoyado por metodologías y estándares. Si no, correremos el riesgo de realizar acciones puntuales

Por lo tanto, la seguridad no debe ser percibida como una cuestión meramente tecnológica y, se ha de abordar como una estrategia con una visión global que comienza haciendo un análisis de las características del negocio para determinar, posteriormente, qué tecnologías están disponibles para dar apoyo a la estrategia que se ha definido anteriormente.

Por eso es importante trabajar la seguridad como un proceso, estructurado, apoyado por metodologías y estándares (como, por ejemplo,

ISO 17799:2005 - Código de buenas prácticas para la Gestión de la Seguridad de la Información; este estándar es el modelo de seguridad seguido por IBM en sus proyectos y forma parte de la formación de sus profesionales del área de Seguridad).

A modo de ejemplo, IBM cuenta con un Documento de Controles de Seguridad de la Información (denominado GSD331) que acuerda y revisa con cada cliente cuando se externaliza la gestión de su entorno tecnológico; y, además, IBM pone a disposición del mercado un marco de mejores prácticas para el área de seguridad, denominado IBM Information Security Framework.

Figura 1
Estrategia de seguridad.

El uso de estos modelos y marcos normativos constituye uno de los pasos a abordar dentro del proceso de Seguridad. Si no abordamos la seguridad como un proceso corremos el riesgo de realizar acciones puntuales sin que éstas tengan una visión de conjunto o hacer una aproximación parcial muy orientada a la tecnología y no al resto de áreas de la organización (roles, responsabilidades, procesos, etc.).

El proceso de despliegue de la seguridad se establece teniendo en cuenta los aspectos de negocio, que permitirán establecer prioridades y requerimientos, y, por otro lado, los condicionantes organizativos y tecnológicos, que establecerán las capacidades para el despliegue de seguridad.

Partiendo de estos condicionantes, se propone un ciclo que siga las siguientes etapas:

• Es importante iniciar el ciclo con **un análisis de riesgos** que identifique cuáles son los activos de información críticos para el negocio. Se trata de analizar el entorno de seguridad y los riesgos que lo amenazan, para así poder saber qué elementos se debe proteger.

• Sabiendo lo que se debe proteger, el siguiente paso es establecer una **política de seguridad** que determine cómo se deben proteger los activos.

• Sabiendo qué se debe proteger y cómo, ahora se debe plantear con qué **mecanismos** poder llevar a cabo lo recogido en las políticas definidas en el paso anterior. Conviene recordar que no sólo se debe pensar en mecanismos tecnológicos; no hay que olvidar mecanismos organizativos (personal dedicado a seguridad, procesos de seguridad, etc.), documentales (procedimientos, informes, etc.), entre otros muchos.

• El cuarto punto del ciclo es la **fase de implantación y gestión**. Se trata de poner en marcha, bajo un correcto marco de gestión, los mecanismos definidos en el paso anterior.

• **Revisión y auditoria** para identificar puntos de mejora para evolucionar y potenciar el proceso global de seguridad.

CICLO CONTINUO

Conviene resaltar la importancia de que la estrategia de seguridad sea considerada como un ciclo continuo, siempre activo. Se trata de que sea un proceso evolutivo que, de forma permanente, detecte puntos de mejora.

Es fundamental abordar la seguridad como un proceso de mejora continua ya que es necesario estar atento a nuevas necesidades y nuevas capacidades, que deben ser contempladas dentro del ciclo para analizar qué nuevos mecanismos se deben poner en práctica, y acometer su inclusión en la estrategia de seguridad corporativa. En el mundo de los negocios actual lo único seguro es el cambio. Por esta razón es necesario dar un paso más y abandonar la percepción actual de la seguridad como un entorno estático de protección y abordar la seguridad como un elemento con capacidad para dar respuesta a un entorno cambiante y dinámico.

CONCLUSIÓN

A pesar de los mensajes alarmistas que a menudo se divulgan, podemos asegurar que en este momento las empresas españolas han iniciado un proceso hacia la madurez, en lo que ha seguridad se refiere. El que una organización consiga generar un alto grado de confianza entre sus clientes, empleados, accionistas, etc. depende en gran medida de cómo se aborde la seguridad. Para IBM la clave del éxito reside en tratar la seguridad como un proceso apoyado por metodologías y con influencia en toda la organización.

A la hora de abordar el área de la seguridad se debe tener una visión global que abarque todos los elementos que cubre la seguridad. Esta visión no debe centrarse sólo en los aspectos tecnológicos, puesto que la implantación de las más modernas tecnologías no garantiza por sí sola la seguridad de una empresa. Hay que establecer una estrategia que comience haciendo un análisis para identificar los elementos a proteger y los riesgos que los amenazan. Posteriormente, una vez que se hayan establecido las políticas de

seguridad es cuando se decide cuáles son las tecnologías a implantar.

Es necesario hacer constar que, en este momento, existen en el mercado tecnologías válidas y aplicables para cubrir y satisfacer los requerimientos de seguridad de la información, y poder evitar, minimizar o paliar el impacto de los riesgos detectados. Pero aún estando la tecnología disponible, no todas las organizaciones hacen un uso adecuado de ella. La clave de una correcta estrategia de seguridad está en afrontar la seguridad con la mayor amplitud posible (para no olvidar ningún aspecto relevante), haciendo uso de estándares y metodologías que nos permitan llevar a cabo un despliegue formal y estructurado, que mantenga activo el proceso de manera continua.

Notas

[1] Autor de Contacto: IBM, C/ Santa Hortensia, 26-28; 28002 Madrid (España).