



¿FALTAN FABRICANTES?

Quizás el título de este artículo despiste a muchos de los lectores de SIC, pues todos sabemos que en los últimos años el mercado de la seguridad se está fusionando mes a mes. Las empresas han invertido mucho dinero en proteger el perímetro, las aplicaciones, los datos, los dispositivos móviles, etc.; y aún así, nos sigue faltando algo. Todos los que consumimos/generamos servicios de seguridad deseamos que existan proveedores de soluciones, integradas, fáciles de implantar e innovadoras; y sorprende ver la cantidad

Es posible que la crisis nos permita agudizar el ingenio para hacer más con menos. Son momentos en los que debemos intentar optimizar las tecnologías incorporadas, mejorar los procesos e impulsar con mayor dedicación y recursos la educación de las personas.

de presentaciones, folletos, eventos... donde se ofrecen soluciones tecnológicas; sin embargo, muy pocos son los que vienen a ofrecer "ayuda" para mejorar la conciencia de seguridad y educación de nuestros usuarios/clientes, quienes, al fin y al cabo, se han convertido en el eslabón más débil.

En los temas de seguridad de la información, como en muchos otros, deberíamos basarnos en los tres pilares fundamentales que la soportan: la tecnología, los procesos y las personas. Hoy la realidad nos muestra que nos hemos ocupado fundamentalmente del pilar de la tecnología, en menor medida del pilar de los procesos y en escasa o nula dedicación al de las personas. En España, el porcentaje de presupuesto que las empresas dedican a la concienciación de la seguridad, respecto del total del presupuesto dedicado a la seguridad, es insignificante.

Existen teorías que justifican esta situación argumentando que la tecnología ha evolucionando a un ritmo bastante intenso y las empresas no siempre han podido implantar programas de formación para enfrentar esos cambios, provocando que se creen y/o fortalezcan malos hábitos en el ámbito de la seguridad.

Desafío

La tecnología es necesaria, pero no suficiente y quienes tenemos la responsabilidad de llevar adelante las funciones de seguridad de la información debemos cambiar esa tendencia actual. Ése es nuestro desafío y, para lograrlo, tenemos que implantar programas de concienciación de seguridad, basados en las políticas corporativas y con un adecuado proceso de seguimiento y continuidad, y cuyo objetivo sea hacer comprender a los usuarios

la responsabilidad que tienen respecto a la seguridad de la información. Es imposible creer que haremos más seguras nuestras compañías sólo con el esfuerzo y dedicación de las áreas especialistas.

Este desafío es mucho más difícil de superar que implantar soluciones tecnológicas, dado que involucra a un variado número de Direcciones/Departamentos

no constituye una excepción. Debemos ayudar al usuario a adaptarse al cambio e incorporarse activamente a él. Será fundamental transmitir **qué** hay que proteger, **por qué** y **cómo**.

- **Es responsabilidad de todos.** Se debe de transmitir que las áreas de seguridad de la información no pueden afrontar dicho reto sin el compromiso de todos.

- **Diferenciación de la audiencia.** Aunque el programa debe de ser único, hay que segmentar los contenidos clave y niveles de profundidad según las funciones de las personas en la compañía. Hay que sensibilizar a los mandos directivos, concienciar a los mandos medios y formar a los niveles operativos.

- **Continuidad.** Crear una cultura de seguridad de la información en una empresa necesita dedicación y tiempo. Por eso, aquellos planes que no tengan una visión a largo plazo fracasarán.

Conclusiones

Es posible que la crisis en la que estamos inmersos, nos haga reflexionar sobre el pasado y nos permita agudizar el ingenio para poder hacer más con menos. Son momentos en los que debemos intentar optimizar al máximo las tecnologías incorporadas, modificar los procesos para mejorarlos y obviamente impulsar con mayor dedicación y recursos a las

En España, el porcentaje de presupuesto que las empresas dedican a la concienciación, respecto del total del presupuesto dedicado a la seguridad de la información, es insignificante.

de la empresa, más allá de los dedicados a las tecnologías.

Sabemos que no es un camino fácil de recorrer y algunos de los problemas que deberemos superar seguramente serán:

- **Compromiso Directivo.** Es necesario sensibilizar a los niveles directivos. En esta tarea es fundamental apoyarse en los Comités de Seguridad de la compañía. Afortunadamente, en los últimos años los niveles directivos están cada vez más sensibilizados por estos temas.

- **Rechazo al cambio.** "Lo único inmutable es el cambio", y nuestro sector

grandes olvidadas, las personas.

Termino con dos frases de Bruce Schneier: "Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología". Y para rematar: "La seguridad de la información es un asunto de personas, procesos y tecnología". ■



Alejandro Villar Assenza-Parisi
Jefe de Seguridad de la Información
REPSOL YPF