ESTUDIO 'CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN'

La **seguridad** es **cosa** de **todos**

Texto
R. Contreras

La tecnología de protección ha avanzado y se han desarrollado políticas de buenas prácticas para minimizar los incidentes de seguridad. Pero las empresas siguen teniendo el 'enemigo' en casa, el eslabón de la cadena que por desconocimiento, testadurez o intencionadamente no cumple con las normas que dicta el sentido común y abre la puerta a posibles infecciones y ataques que pueden causar estragos en la información corporativa. Por suerte las empresas españolas empiezan a ser conscientes de este hecho y están poniendo en marcha planes de concienciación para sensibilizar a sus empleados de la necesidad de adoptar una política de seguridad. Para medir el avance que

están realizando las empresas españolas en este camino, Autelsi ha realizado el estudio 'Concienciación en Seguridad de la Información', que ha dado como corolario un decálogo que se resume en dos principios básicos: innovar en los mensajes para conseguir la involucración de todos los integrantes de la empresa y el patrocinio de la alta dirección.

Desde Autelsi se insiste en estos aspectos: "la seguridad de la información ha de ser entendida como un todo, pero hay un componente que se repite y no depende de definiciones ni metodologías: las personas de la organización". Y la concienciación pasa por "conseguir un nivel adecuado de conocimiento por parte de cada empleado de la organización de las normas aplicables en la misma que ayuden a conseguir el nivel de seguridad de la información que su empresa necesita".

El estudio refleja que el 97% de las empresas cree necesario realizar acciones de concienciación, si bien solo el 34% de las mismas tiene un proyecto en marcha. Un 46% de las organizaciones consultadas asegura que va a poner un plan en prueba. En cuanto a la distribución de estándares de buenas prácticas, es atinado pensar que el 30% del Esquema Nacional de Seguridad (ENS) correspondería básicamente al sector público, mientras ISO 27001 tiene mayor difusión en el ámbito privado.

¿Pero qué motiva a las empresas a desarrollar este tipo de planes? Autelsi destaca cuatro aspectos condicionantes: los usuarios cuentan con nuevos dispositivos; la evolución de las incidencias de seguridad; los cambios en el entorno de interconexión y las modificaciones en la regulación. La continuidad de negocio ocupa la quinta posición, porque representa una toma de conciencia de los encuestados en torno a la estrecha conexión de la concienciación con la reputación corporativa.

Los departamentos más implicados en estas campañas de concienciación son, por este orden, Seguridad, IT y Recursos Humanos, frente a una escaso protagonismo de la dirección y del departamento de legal.

Como opinión generalizada, la intranet corporativa es una herramienta muy útil en el programa de concienciación. Su rol como elemento oficial para la comunicación entre la organización y el personal que se desempeña en ella hace que, de forma intuitiva, las personas busquen espontáneamente en ella información y recursos de todo tipo. Así, ofrece la posibilidad de ofrecer contenidos y elementos previstos en el programa de concienciación. No obstante, todos reconocen que se trata de campañas complejas, con muchos desafíos personales y que tocar la fibra emocional es la clave para conseguir que se vaya progresando en esta ardua tarea. ■

"La seguridad debe ser contemplada como un todo, pero siempre se repite un factor: las personas"

Buenas prácticas para concienciar en la seguridad

1. Establecer la necesidad y el por qué
2. Definir un plan, una estrategia y trabajarla
3. Involucración y patrocinio de la alta dirección
4. Equipo multidisciplinar
5. Apoyarse en Recursos Humanos
6. Seleccionar temáticas en las que es necesario concienciar
7. Cuidar el mensaje que se transmite: Innovar
8. Estudiar los canales adecuados
9. Refuerzo/actividad constante

Fuente: Autelsi

COMITÉ DE SEGURIDAD DE **MEDIASET**

Creatividad y protección

En Mediaset la concienciación de la seguridad TIC ha ido madurando a medida que se definía una estrategia de seguridad: "se pasó de gestores de protección de datos a un comité de seguridad; de planes de formación comunes a planes de formación personales", todo ello motivado por el cumplimiento regulatorio y la inquietud por los entornos cambiantes, como explica Ramón Ortiz González, Responsable de Seguridad de Mediaset España.

El comité de seguridad se creó en 2007 con el fin de dar a conocer la normativa reguladora y los procedimientos a seguir y se llegó a la conclusión de que los destinatarios tenían que ser todos los empleados, incluyendo proveedores externos y productoras asociadas. En este comité estaban implicados la división de tecnologías, dirección de auditoría interna, asesoría jurídica, responsable de seguridad informática, asesoría jurídica, el CISO y el responsable de seguridad física. "Entre sus atribuciones se encuentran velar por el cumplimiento de la política de seguridad y del código ético y facilitar a los empleados procedimientos y planes de formación", detalla Ortiz.

Estos planes de formación tienen como misión alfabetizar para la reducción de incidentes y crear una cultura de detección del riesgo poniendo en alerta al usuario. "Todo ello redunda en la mejora de la imagen de Mediaset ante sector y afectados", puntualiza el CISO. Los temarios se reparten en tres capítulos: fijos (cumplimiento y procedimiento); temporales (ciberriesgos, proyectos IT…) y tendencias (redes sociales, teletrabajo, consumerización).

Ortiz enumera los diferentes formatos que pasan por la formación presencial, videoconferencia entre delegaciones; campañas de marketing (intranet y campañas de e-mail); campañas de medios y web; reglas de comportamiento para el público asistente a los platós y certificaciones para los colaboradores externos.

Aprovechando su plataforma audiovisual, Mediaset ha podido ser creativo emitiendo programas monográficos como el de 'Tor, la red invisible', propiciando encuentros digitales con directores de la agencia, dando cobertura en informativos y series de temas sobre seguridad y lanzando campañas publicitarias, como la de 'doce meses, doce causas', que versaba de la privacidad en las redes sociales.

RAMÓN ORTIZ GONZÁLEZ | Responsable de Seguridad de Mediaset España

> **"Se pasó de gestores de protección de datos a un comité de seguridad; de formación común a formación personalizada"**

La Red Tor y Deep Internet

En agosto de 2014, el programa de Mercedes Milá, 'La Redacción', se sumergió en la Deep Web. Un reportero se infiltró en el lado más oscuro de la red para investigar qué se puede encontrar y cómo se puede conseguir. Una muestra exitosa de la política de difusión sobre la seguridad que aplica Mediaset.

CAMPAÑA DE CONCIENCIACIÓN DE **RENFE**

Sensibilizar y concienciar

FRANCISCO LÁZARO I
CISO de Renfe Operadora

Para Francisco Lázaro, CISO de Renfe Operadora, hay que distinguir entre dos conceptos que en muchas ocasiones se confunden: sensibilización y concienciación. "Sensibilizar es tener constancia de una situación y concienciar es actuar en consecuencia". Lázaro observa dos comportamientos derivados de la "gente que desconoce la seguridad y la que se opone a las medidas de seguridad. Hay profesionales del área de Tecnologías de la Información que no ayudan con sus ocurrencias". El responsable de seguridad de Renfe remite a una conclusión lapidaria de Bruce Schneier, en su libro 'Secrets and liers': "si piensas que las TI pueden resolver tus problemas de seguridad, entonces no entiendes el problema y tampoco entiendes de tecnología".

Siguiendo este argumentario, Lázaro establece un axioma contradictorio, el ser humano es confiado por naturaleza y las empresas tienen que ser desconfiadas por supervivencia; "la razón de ser de la desconfianza de las empresas es la necesidad de generar confianza (en sus clientes, en sus socios, accionistas, empleados y sociedad en general). Este conflicto derivado de estas dos posiciones antagónicas solo puede ser superado cambiando comportamientos".

"La gente pierde el norte, lo que puede estar bien en la vida personal, no lo está en la vida profesional" y alude a un selfie que se hizo durante una operación en un hospital chino, en el que todos los ayudantes y enfermeras posaron estúpidamente ante la cámara mientras el cirujano se empleaba a fondo con su tarea.

Dada esta naturaleza, las cuatro fases lógicas de Renfe se basan en sensibilizar, concienciar, formar y capacitar. Su forma de atajar las incidencias es yendo directamente al usuario implicado y "ser agresivo con las consecuencias que pueden sufrir mediante casos acaecidos a otras personas. Cuando tocas su fibra personal se dan cuenta de que son vulnerables y, a partir de ahí, ya puedes formarles". Entre las principales acciones que realizan, Lázaro enumera: píldoras formativas inspiradas en Incibe para explicar qué son los agujeros de seguridad o el phishing; guías de uso; acciones de campo (teoría, demos, plano personal); acciones especiales de concienciación a colectivos (teoría, demos, plano personal); monitorización de resultados y simulación de resultados.

> **"El hombre es confiado por naturaleza y las empresas tienen que ser desconfiadas por supervivencia"**

Bruce Schneier, en su libro **'Secrets and liers',** sentencia: *"si piensas que las TI pueden resolver tus problemas de seguridad, entonces no entiendes el problema y tampoco entiendes de tecnología".*

CAMPAÑA DE CONCIENCIACIÓN DE **REPSOL**

El factor humano

La multinacional petrolera española integraba su área de seguridad dentro de producción, hasta que en 2011 pasa a depender del CIO y un año después se activa un plan de concienciación. "Se empieza a pensar en el negocio y los usuarios, que vivían en una 'feliz ignorancia' asistidos por sus guardianes los técnicos de seguridad", relata Juan Francisco de Dios Oviedo, gerente de Ciberseguridad de Repsol. Esta primera aproximación se basó en la normativa, lo cual generó desgana y no tuvo aceptación por parte de la plantilla.

"Decidimos rediseñar la campaña y centrarnos en la gente, poniendo acento en el sentido común. Es necesario que el profesional tenga suficientes conocimientos y ser consciente de la importancia de la seguridad de la información", argumenta Oviedo. Las iniciativas fueron ingeniosas, "se dispersaron sobres con el sello 'confidencial' y más de un incauto lo abrió llevándose la sorpresa de recibir un mensaje de alerta y una alusión a su irresponsabilidad". De la misma manera, con la complicidad de RRHH, se lanzaron correos con phishing exagerado en el que también picaron algunos ingenuos.

También se crearon los '10 momentos de la verdad', explicaciones de no más de tres minutos, contando casos muy concretos como configurar una WiFi para que no pueda ser hackeada.

"Hemos hecho labores de acercamiento a los departamentos, mediante un catálogo de servicios de ciberseguridad. La gente de negocio no entendía nuestro lenguaje, ahora les hablamos de problemas como fraude o fuga de información, y no de las herramientas que están por debajo", continúa.
Otras acciones han sido igual de imaginativas: salvapantallas con carácter recordatorio, cartelería digital en tres idiomas, vídeos humorísticos llamando a la responsabilidad, con títulos tan disparatados como 'Datólicos anónimos' o 'El señor de los permisos', que obtuvieron buena acogida.

Como conclusión, el directivo se felicita por la implicación de la dirección que apoyó con un presupuesto y la creación de un nuevo comité. En la parte negativa, Oviedo considera que los canales de comunicaciones habituales están agotados: "el correo electrónico está saturado y lo que mejor funciona es el boca a boca".

JUAN FRANCISCO DE DIOS OVIEDO | gerente de Ciberseguridad

"La gente de negocio no entendía nuestro lenguaje, ahora les hablamos de problemas"

Nivel de seguridad =
(Cn+ Ds+ Gi+ Av + Act) x Sc

Cn *Cuadro normativo*
Ds *Desarrollo seguro*
Gi *Gestión de identidades*
Av *Antivirus*
Act *Actualización de sistemas/ Aplicaciones*
Sc *Sentido común de los usuarios*

NECESIDADES
Agotamiento de los canales tradicionales

SOLUCIÓN
Implicación de la alta dirección y presupuesto