Verano, mejor momento para analizar tu respuesta ante una brecha de ciberseguridad

Con la llegada del verano y aprovechando que gran parte del personal está de vacaciones, es el momento oportuno para el chequeo de los niveles de madurez de ciberseguridad en tu empresa. Sin embargo, por lo general las empresas sólo se preocupan de estas tareas cuando se enfrentan a una situación caótica de fuga de información, el teléfono ardiendo de llamadas y con la presión interna de dar una solución urgente al conflicto. Así que no existe momento mejor que el presente para preparar a la empresa para una situación de brecha de seguridad, fuga de datos, o fallo en el sistema de seguridad, es decir, es el momento de **diseñar la estrategia de ciberseguridad** de tu empresa.

Tras analizar el reciente informe de *Global Information Security Survey* de Ernst & Young, se evidencia que las organizaciones no están preparadas para este tipo de amenazas. Según dicho informe, el **56% de las organizaciones dice haber**

hecho ya cambios en sus estrategias de negocio para contemplar los riesgos que representa las ciberamenazas. Sin embargo, tan solo el 4% de las organizaciones confían en que han tomado en consideración toda la información sobre las implicaciones en seguridad de sus actuales estrategias. Además, el **35% de los encuestados describe sus políticas de protección de datos como muy limitadas o inexistentes**. Esto genera un gran problema, ya que según el actual Reglamento General de Protección de Datos (RGPD), las empresas deberían notificar las brechas de seguridad sufridas en un plazo de 72 horas una vez detectadas. Sin embargo, solo el **17% de las empresas confiesa que lo notificaría a sus clientes en ese periodo.**

Así que aprovecha momentos de menor actividad en tu empresa para tomarte un tiempo y reflexionar sobre cómo proteger tus activos, valorar el nivel de madurez de ciberseguridad de tu empresa y realizar un Plan Director de Ciberseguridad.

Y si no sabes cómo empezar, aquí van algunos consejos.

Estrategia de comunicación a la hora de provocar una brecha o incidencia en ciberseguridad.

Recientemente hemos visto importantes organizaciones cuyo departamento de comunicación no ha sabido manejar situaciones de crisis debidas a ciberataques. Ante estos incidentes, es preciso salir a los medios, contactar o comunicar con los clientes, informándoles puntualmente de la brecha y de cómo les afecta. Aunque parezca sorprendente, este punto es muy delicado y requiere ser pensado con mucho cuidado, asesorado por el gabinete jurídico de la empresa. Por lo que es más que **recomendable disponer de una serie de plantillas o cartas modelos que permita comunicar de** una forma responsable y correcta a los interesados, además de la Agencia Española de Protección de Datos, si corresponde.

Recuerda que **los clientes perciben los agujeros de seguridad como una brecha en la "confianza" con su proveedor**, por lo que el cómo lo comunicas es fundamental para no dañar más la reputación de la empresa.

Planifica un canal de comunicación con tus clientes.

Los clientes son tu activo más importante, por lo que hay que procurar mantenerlos informados en todo momento mediante un canal. Dicho canal puede

ser una red social o una página web preparada y mantenida offline para activar en el momento que más haga falta. Esto evitará que el departamento IT invierta tiempo y energía en informar a los clientes mientras deberían solucionar la situación de urgencia en sí.

Protege a tu cliente

Si hay una brecha de seguridad que afecte a tu cliente, es necesario tener una serie de recomendaciones para proteger sus datos. Por ejemplo, recomienda a tus clientes medidas para mejorar la seguridad de sus cuentas activando la autenticación en dos factores, fortaleciendo sus contraseñas, etc.

Pon a prueba tus sistemas de seguridad

Es hora de mirar esas copias de seguridad que se hacen desde hace años y que, por suerte, nunca tocó usarlas. De modo que, con anticipación, intenta restaurar una. Responde a preguntas como ¿la copia de seguridad realmente copia todas las carpetas o no se toca desde hace meses y la lista de directorios ha crecido? Si un Ransomware cifra todos tus servidores ¿existen copias de seguridad offline para recuperar los datos?

Recuerda: Hasta que no pongas en práctica estas ideas, nunca sabrás la eficiencia de respuesta ante emergencias de tu empresa. Y si necesitas apoyo, siempre puedes contar con empresas especializadas como Hardening de empresas que estarán dispuestos a ayudarte.

Para el cibercrimen no hay negocios ni muy grandes ni muy pequeños para atacar. Todos son objetivos rentables.