Publicado en MADRID el 30/11/2018

# 7 consejos de VASS para evitar un ciberataque en una empresa

## De los 120.000 ‘hackeos’ que se produjeron el año pasado en España, un 70% los sufrieron las pymes

Según el Instituto Nacional de Ciberseguridad de España (Incibe), España registró el año pasado su récord en ciberataques, con un total de 120.000 incidentes. De ellos, un 70% tuvieron como objetivo las pequeñas y medianas empresas, por lo que la prevención se convierte en imprescindible para hacer frente a los hackers.

Con motivo de la celebración, este viernes 30 de diciembre, del Día Internacional de la Seguridad de la Información, la consultora especialista en soluciones digitales VASS ha elaborado una práctica lista con los 7 consejos que toda organización debería tener en cuenta para evitar un ciberataque: Usar contraseñas seguras: cuando se tienen claves y códigos para casi todo (desde el móvil hasta la maleta), el uso correcto de una política de contraseñas se torna vital para cualquier empresa. Deberían ser normas de obligado cumplimiento la renovación de las mismas de forma periódica, el uso de caracteres especiales y evitar incluir información personal relacionada con el usuario.

Evitar accesos no deseados a la información: desgraciadamente, las pérdidas o robos de dispositivos están ahí y no se pueden minusvalorar esos riesgos. También los intentos de accesos no adecuados, por eso, lo mejor es hacer un cifrado de la información en portátiles y móviles, así como cifrados de información tanto en el disco del ordenador como los backups. Ya se sabe: organización precavida, vale por dos.

Proteger la información en dispositivos móviles: cada vez más se accede a la información corporativa a través de móviles, sean de empresa o personales. Se hace imprescindible, por tanto, que los usuarios tomen conciencia de la información corporativa que portan en sus dispositivos y la importancia de controlar el acceso a ella mediante huella, pin u otros mecanismos que la protejan. Nunca estará de más, por ejemplo, que las empresas establezcan medidas de seguridad a nivel de acceso, instalación de aplicaciones y cifrado de la información en los en los móviles que ofrece a sus trabajadores o incluso utilizar, de forma eficiente, el control de acceso al dispositivo personal en caso de existir información de la empresa en él.

Proteger la información ante miradas indiscretas: sin darnos cuenta, consultamos emails, cuentas o documentos confidenciales en el metro, en una cafetería, en la estación de tren o en el aeropuerto sin percatarnos de quién puede estar mirando, aunque sea de soslayo, la pantalla. Así que, ojo, nunca mejor dicho, con las indiscreciones.

Publicar información sensible en foros no adecuados: todas las empresas u organizaciones deberían establecer normativas para la publicación de asuntos internos (aunque sean más o menos públicos) en foros no adecuados al tipo de información divulgada. Y, sobre todo, concienciar a sus trabajadores de

que, en plataformas como las redes sociales o los servicios de mensajería instantánea, se puede perder el control de una comunicación.

Formar y concienciar: nadie nace sabiendo, de ahí que la formación y concienciación en seguridad deban de estar incluidas en los planes de formación, cultura empresarial, políticas y normativas de cualquier organización. Es algo necesario que, sin embargo, con más frecuencia de la deseada, se olvida o se posterga sine die.

Aplicar el sentido común y fomentar la paciencia: quizás sean los aspectos más complicados por cuanto que son los más obvios, pero ambos son de vital importancia para cualquier política de seguridad de una empresa. Las reglas básicas de la seguridad son: actuar con cautela a la hora de publicar información, no aceptar correos electrónicos de remitentes no conocidos y poner en conocimiento cualquier sospecha con los responsables de seguridad de la empresa.

Para José Manuel de la Puente, Gerente de Seguridad de VASS, con la puesta en marcha de estos consejos y teniendo presentes las citadas advertencias se podrían prevenir gran parte de los ciberataques a los que, hoy día, están expuestas las empresas españolas. Principalmente, tal y como señala este especialista en seguridad, porque, “en muchas ocasiones, es la pérdida de consciencia en torno al riesgo de ser ‘hackeado’ la causa de estos ataques a través de la red y que pueden ocasionar, según la dimensión de los mismos, pérdidas millonarias”.

España, según el estudio ‘Norton Cyber Security Insights Report 2018’, es el tercer país que sufre más ataques online (tras Estados Unidos y Reino Unido) y al menos un tercio de la población ha sido víctima de un ciberataque, lo que se traduce en pérdidas de más de 2.000 millones de euros. No es de extrañar, por tanto, que en el actual entorno de creciente manipulación digital, robo masivo de datos, fraudes online y de ataques virtuales aleatorios, la ciberseguridad sea uno de los asuntos prioritarios para la Comisión Europea, que ya ha establecido programas marco de I+D para luchar contra las ciberamenazas.

**Datos de contacto:**
ANA VAZQUEZ

Nota de prensa publicada en: MADRID

Categorías: E-Commerce Ciberseguridad Recursos humanos Otras Industrias