

Las 7 claves para evitar ciberataques en las empresas según Hasten Group

La seguridad en los sistemas y comunicaciones empresariales son una prioridad y necesidad. Las siete claves para protegerse de los ciberataques según Hasten Group y el papel decisivo del hacking ético

La conexión a internet, las nuevas tecnologías y las comunicaciones en la actualidad son necesarias imprescindibles para realizar la mayoría operaciones comerciales, alcanzar nuevos mercados e impulsar las eficiencias que benefician a los clientes y a la sociedad. Las empresas en sus operaciones están expuestas a numerosos riesgos y fallos en ciberseguridad, muchos criminales competidores desleales y hackers aprovechan las debilidades de las tecnologías de la información para acceder a las empresas.

La seguridad digital es una prioridad, las empresas deben adoptar medidas preventivas que garanticen el almacenamiento, gestión y transmisión de la información al convertirse esta en un objetivo de los ciberdelincuentes. La amenaza tecnológica es una realidad, las empresas y las organizaciones necesitan un sistema de seguridad informática que les proteja de los constantes peligros y ataques cibernéticos, que además de una gran pérdida económica, mala reputación y vulneración de todo su sistema productivo e información existente pueden ocasionar una notable pérdida de ventas y de clientes. Las empresas necesitan protegerse; si no disponen en su plantilla de personal cualificado debido a su reducido tamaño o por otras cuestiones debieran externalizar este servicio para protegerse de posibles ataques cibernéticos.

Desde HastenGroup, consultora tecnológica especializada en el desarrollo de aplicaciones multiplataforma, señalan por su experiencia en diferentes proyectos con los clientes 7 claves decisivas para proteger a las empresas y a las organizaciones.

La primera, asegurarse de proteger los datos obrantes, especialmente aquellos sensibles y comprobar la información y correos de desconocidos. Evitar contraseñas comunes. Utilizar contraseñas fuertes y robustas lo más larga posible, al menos ocho caracteres, que combine caracteres alfanuméricos, utilizar mayúsculas y minúsculas y que incluyan caracteres especiales; asimismo conviene cambiar de contraseña con cierta periodicidad.

Ser conscientes de la posibilidad de sufrir un ciberataque, los empleados deben estar advertidos de los riesgos de un ataque, es necesario evitar que comentan errores comunes. La empresa contará con un plan de comunicación para actuar en situaciones de crisis, como por ejemplo sufrir una amenaza. Realizar análisis periódicos internos en el servidor, a ser posibles diarios y también monitorear y revisar la actividad que se realiza en la red.

Restringir el acceso a los equipos, restringir acceso a aquella información que no necesiten, así como inhabilitar los accesos desde varios sistemas, porque puede ser la puerta de acceso de un hackers. No

permitir que personas ajenas utilicen los equipos. Proteger todos los dispositivos conectados con herramientas eficaces y mantenerlas actualizadas periódicamente. Y por último, realizar copias de seguridad de todo para prevenir ataques cibernéticos y poder restaurar en caso de vulneración del sistema. Hoy en día la nube ofrece servicios no sólo de almacenamiento de datos sino para proteger la seguridad de la información y garantizar la privacidad.

HastenGroup ofrece un servicio eficaz de ciberseguridad a las empresas para evitar riesgos cibernéticos. Este servicio: Seguridad para sus Sistemas y Comunicaciones consta de una consultoría previa de sus sistemas y comunicaciones; en segundo lugar, suministro, instalación y puesta en producción de un firewall de nueva generación, que refuerza la seguridad perimetral de sus Redes y Sistemas; a continuación realiza test de intrusión desde el exterior a su red y sistemas de información o hacking ético, después lleva a cabo la protección de los equipos de usuario y, por último, la monitorización remota de redes y seguridad facilitando a las organizaciones y empresas tener todo el control de sus activos corporativos. El servicio de hacking ético que ofrece HastenGroup es una prueba de intrusión externa, donde un hacker tras la aprobación de la prueba y sin recibir más información que una dirección de IP o nombre de dominio pretende tomar el control de la red y conseguir información de los sistemas. El papel del hacking ético, afirman en HastenGroup “es decisivo, clave y positivo para evaluar los posibles riesgos informáticos, fortalecer, mejorar la seguridad y prevenir ataques informáticos porque es capaz de identificar todas las brechas de seguridad y proporcionar soluciones para cada una de ellas.”

Hasten Group: Consultora española, que nace en 2015, fruto de la fusión por absorción de dos empresas tecnológicas que reunían más 10 años de experiencia en el campo del desarrollo de aplicaciones móviles y web, con el objetivo de consolidarse como proveedor de confianza de servicios tecnológicos para empresas. Actualmente, cuenta con más de 100 profesionales. Ha participado en más 60 proyectos desarrollando su actividad en diferentes sectores: finanzas, telecomunicaciones, utilities, administración pública, sanidad, energía, formación o turismo. Está homologada por las más importantes multinacionales tecnológicas y financieras y representa un nuevo concepto en la búsqueda de la “especialización integrada” apostando por la eficiencia en profesionalización y gestión. <https://www.grupohasten.com>

Datos de contacto:

En Ke Medio Broadcasting
912792470

Nota de prensa publicada en: [Madrid.- EKMB](#)

Categorías: [Franquicias Finanzas Emprendedores E-Commerce Software Ciberseguridad](#)

NotasdePrensa

<https://www.notasdeprensa.es>