Publicado en Madrid el 29/11/2019

Los 3 ciberataques que, según VASS, seguirán siendo motivo de preocupación en 2020

VASS hace repaso de los principales ataques informáticos que han proliferado en 2019 y que habrá que seguir vigilando de cerca durante el próximo año. La empresa líder en soluciones digitales ofrece fórmulas efectivas para evitar estos ciberataques que, en 2018, afectaron en más de 30.000 ocasiones a empresas estratégicas y organismos públicos en España

Ser víctima de un ciberataque sigue siendo una de las principales preocupaciones de los directivos y ejecutivos de las empresas, en especial, de las empresas de interés estratégico que, junto a las entidades de la Administración Pública, constituyen el principal foco de acción de los hackers.

De hecho, el año pasado, se registraron más de 33.000 incidentes relacionados con la ciberseguridad en nuestro país en este tipo de organizaciones, suponiendo un aumento con respecto a 2017 del 25%, según el informe 'Incidentes de ciberseguridad industrial en servicios esenciales en España', elaborado por el Centro de Ciberseguridad Industrial (CCI) y Checkpoint.

La diversificación de estos ataques informáticos y la continua aparición de nuevas formas de ciberdelitos dificultan, cada vez más, su control y prevención a los departamentos dedicados a la seguridad informática.

Por ello, y con motivo de la celebración este sábado 30 de diciembre del Día Internacional de la Seguridad de la Información, la empresa líder en soluciones digitales VASS quiere hacer repaso de los 3 principales ciberataques que han proliferado durante este año y a los que habrá que seguir prestando mucha atención en 2020. Estos han sido:

?1.Malware o software malicioso. De estos ataques, hay varios tipos:

Virus: Es un software que infecta los archivos del sistema. Es necesario ejecutarlo desde el lado de los usuarios.
Troyanos: Es similar al virus, pero su función es permitir el acceso a otros programas maliciosos a través de puertas traseras.
Spyware: Son programas espía que buscan obtener información.
Ransomware: Se trata de un secuestro de datos, encriptándolos y solicitando un rescate por ellos.

2.Phising: es la obtención de datos privados, como contraseñas o cuentas bancarias, para utilizarlos posteriormente.

3.Ataques DDos: son ataques de denegación de servicio y consisten en realizar peticiones a un servidor para intentar colapsarlo.
La pregunta ahora es, por tanto, ¿cómo hacer frente a estos ciberataques? Según José Manuel de la Puente, gerente de Seguridad en VASS, la mejor forma para evitarlos es seguir estos consejos:

Contar siempre con antivirus actualizados.
Disponer de software anti-malware y anti-spyware.
Realizar una actualización constante de los equipos.
Contar con un filtro anti-spam para evitar la recepción de correos no deseados
Usar contraseñas seguras: lo ideal es impulsar dentro de la empresa una correcta política de contraseñas, obligando a su renovación de forma periódica, así como a usar caracteres especiales, evitando cualquier relación con información personal del usuario.
Sentido común y paciencia: son dos pilares básicos de cualquier política de seguridad. De hecho, 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 de los responsables de seguridad de la empresa cualquier sospecha que se tenga.
Formación y concienciación: la formación y la concienciación en seguridad deben estar incluidas en los planes de cultura empresarial, políticas y normativas en general como parte de las normas de uso de la organización.
Incremento de la inversión en seguridad.

Datos de contacto:
Redacción
914115868

Nota de prensa publicada en: Madrid

Categorías: Internet Tecnología Digital Seguridad