Publicado en Madrid el 30/11/2022

Retos y amenazas actuales en materia de Seguridad de la Información según Asseco Spain

El ransomware es uno de los ataques más frecuentes y que puede poner en riesgo el negocio o la actividad de las organizaciones. Frente a riesgos en materia de seguridad es necesario disponer de medidas de seguridad adecuadas para prevenir cualquier tipo de vulnerabilidad que pueda generarse en el entorno y sistemas

Actualmente las tecnologías de información y comunicación (TIC) tienen un crecimiento exponencial y que provoca que la superficie de exposición cada vez sea mayor y, en consecuencia, grandes cantidades de información circulan en los medios digitales a diario sin ningún tipo de control.

No hay duda de que esta evolución ha sido favorable y que ha propiciado un desarrollo tecnológico que ha facilitado la vida en muchos sentidos y ámbitos, desde el personal, el académico o el laboral. Ahora más que nunca se cuenta con un sinfín de recursos digitales al alcance, lo cual está al mismo tiempo marcando el desarrollo de las nuevas generaciones.

Más allá de la evolución tecnológica y toda la información disponible y al alcance de cualquiera de la que se dispone, existen grandes retos para su uso adecuado y responsable. Asseco Spain, multinacional de soluciones empresariales IT especializada en ciberseguridad como una de sus áreas de trabajo principales dentro de su core business, reflexiona sobre estos retos/amenazas y cómo se pueden afrontar en el marco del Día Internacional de la Seguridad de la Información, que se celebrará el próximo 30 de noviembre:

Ransomware – Se trata de uno de los ataques más frecuentes y que puede poner en riesgo negocios y organizaciones completas, por lo que la amenaza en relación a la vulnerabilidad de los datos de los demás usuarios es bastante alta. Un ransomware cifra cualquier tipo de información en cualquier dispositivo conectado a una red, incluido los dispositivos IoT (Internet de las Cosas). Por lo que es un malware que fácilmente puede tener un impacto muy grande.

Phishing – Se trata de una técnica de ingeniería social cada vez más popular y extendida entre los ciberatacantes. Se debe estar alerta para no "picar" en este tipo de ciber ataque y así evitar el impacto. Hay que tener cuidado con la información que se comparte y como se comparte.

DDoS - Los ataques de denegación de servicio distribuidos ocurren cuando un sitio web se ve inundado por una avalancha de tráfico, en un corto período de tiempo, provocando su caída. En la mayoría de los casos estos ataques provienen de actores externos, sin embargo, a nivel escolar se ha observado un dato curioso: existe un aumento de ataques DDoS provenientes de alumnos que los compran como servicio en línea para saltarse una clase o examen.

Infección malware: nunca debe estar en las listas de principales ciberataques. Se puede sufrir una infección de software malicioso a través de la navegación por paginas fraudulentas, picando en un phishing,… se debe verificar la seguridad de las páginas en las que se navega, escanear los dispositivos extraíbles (USB, discos externos…),…

¿Cómo se puede luchar contra estas amenazas?
Frente a estos riesgos es necesario disponer de un conjunto de medidas de seguridad que mitiguen dichos riesgos empezando por las capacitación y concienciación de las personas para evitar o reducir la exposición a las vulnerabilidades del alrededor.

¿Cómo se pueden prevenir los riesgos de la privacidad digital?
Según apunta Carlos García Gallardo, Chief Information Security Officer en Asseco Spain, "a nivel empresarial o instituciones será necesario asegurarse de proteger la información la cual es el activo principal de las empresas, organizaciones y las propias personas. De esta manera, aseguraremos la continuidad de la actividad de las organizaciones y la identidad digital de las personas". Además, añade, "para llevarlo a cabo habrá que tener en cuenta medidas tan básicas como tener los sistemas operativos actualizados, tener un buen antivirus, hacer copias de seguridad, cifrar la información, usar VPN´s, etc".

Las empresas tienen un reto constante y papel fundamental en concienciar a sus empleados para que sepan seguir las políticas de seguridad de la empresa y que se de un buen uso de las herramientas internas.

Datos de contacto:
Havas PR
914 56 90 00

Nota de prensa publicada en: Madrid

Categorías: E-Commerce Software Ciberseguridad