los organismos públicos, objetivo de especial interés para los cibercriminales

- **El sector público es uno de los principales objetivos de los ciberdelincuentes.**
- **Los ataques a organismos públicos tienen una motivación económica en el 75% de los casos.**

Las razones que tienen los delincuentes para elegir a los organismos gubernamentales como un blanco de interés están relacionadas habitualmente con la importancia que tiene el servicio que brindan, así como el impacto reputacional que provoca un ataque de esta naturaleza para la opinión pública.

El informe Data Breach Investigations Report (DBIR) 2020 de Verizon contempla una sección específica para las ciberamenazas que afectan en mayor medida a los organismos públicos, y señalando a los ataques a aplicaciones web como el principal problema que sufre este sector. **Los datos están encabezados por ataques de malware, seguido por los activos perdidos y robados**. En el primer caso, el malware habitualmente se descarga por una persona o éste directamente lo instala en el sistema (en un 43% de los casos, este problema surge dentro de la misma organización), lo cual deriva directamente en una brecha de seguridad.

Tal y como sucede en la mayoría de los sectores, un problema habitual de ciberseguridad suele ser la configuración incorrecta de sistemas o servicios (cerca de un 30%). Por otra parte, **estos ataques tienen un objetivo económico, siendo la motivación principal en el 75% de los casos**. Curiosamente, el factor económico ha desplazado al que hasta ahora era la principal motivación en 2019: el espionaje. Los datos de 2020 indican que éste ha bajado en importancia y sólo supone un 19% de los ataques, y que **los datos perdidos durante un ciberataque suelen ser de tipo personal (51%)** o de credenciales (33%).

A los datos aportados por el informe, hay que añadir que si ya en el día a día de cualquier organización, **no es fácil mantenerse actualizado y seguir el ritmo que lleva la tecnología, este hecho es especialmente remarcable en la administración pública**. Sumando a esto que cada día los ciberdelincuentes cuentan con más medios, están más especializados y carecen de limitaciones procedimentales y morales a la hora de llevar a cabo

sus acciones, supone un riesgo cada vez mayor para los organismos públicos y una problemática que debe ser abordada con inmediatez.

Las personas, un eslabón de la cadena a reforzar

Cabe señalar que **igual de importante o más que el despliegue de medidas técnicas, es trabajar la concienciación de los empleados acerca de los riesgos derivados del uso de internet y de las nuevas tecnologías.** Tenemos que partir de la base de que un único clic puede comprometer toda una red, por lo que es necesario que todos los que forman parte de ella sean conscientes de qué tipo de comportamiento irresponsable puede derivar en consecuencias catastróficas. Es por ello que **se hace necesario trabajar en la concienciación de los empleados**, independientemente del ámbito en el que trabajen, y adecuando eso sí las casuísticas de modo que sean comprensibles y útiles para que puedan interiorizarlas y hacerlas suyas.

Cualquier entidad, y especialmente aquellas que tienen un nivel de exposición mayor como es el caso de las pertenecientes al sector público, debe ser consciente de que convive en un mundo donde la tecnología y la amenaza constante de un ciberataque es la "nueva normalidad", por lo que deben adaptar su operativa para poder gestionar el riesgo de la manera apropiada, alcanzando un nivel de madurez óptimo para poder manejarse en este ámbito de incertidumbre.

Desde el BCSC hemos preparado una infografía, con una serie de **recomendaciones para fomentar un nivel de ciberseguridad óptimo de los empleados públicos.** Dichas recomendaciones están agrupadas en los siguientes bloques: el equipo corporativo, las redes sociales, los dispositivos móviles, el correo electrónico y los métodos para compartir la información.

La infografía tiene como objetivo ayudar a que los empleados de organismos públicos adquieran pautas básicas de actuación para limitar el nivel de riesgo al que están expuestos tanto ellos como la entidad para la que trabajan, entendiendo que **todos formamos parte activa del escudo de protección de nuestra organización frente a las ciberamenazas.**

info@bcsc.eus | 945 010 059

Parque Tecnológico de Álava
Albert Einstein. 46-3ª – Ed. E7 01510
Vitoria-Gasteiz