La mejor defensa en ciberseguridad para tu empresa: Formación

El pasado año más del 87% de las empresas experimentó una amenaza de correo electrónico y en torno a un 35% fueron afectadas por un *ransomware*, un programa dañino que secuestra parte de la información del ordenador y que sólo es posible liberar tras el pago de una cantidad económica. La mayoría de las empresas trabajan con información sensible: datos personales de clientes, de proveedores, etc., por lo que se hace más acuciante la protección de estos datos.

Está demostrado que las amenazas que comprometen una organización pequeña, mediana o grande mediante un correo electrónico son una realidad y, lamentablemente, no hay visos de que esto vaya a cambiar. Si bien los sistemas antispam y antivirus pueden resolver a medias la amenaza de este tipo de

correos, en muchos casos nos encontramos que estos correos maliciosos son enviados presuntamente por contactos conocidos mediante suplantaciones de identidad. También se puede dar el caso de que la campaña es tan nueva que los sistemas automáticos como antivirus y antimalwares no la detecta.

El 75% de ataques de *ransomware* se produjo mediante correos electrónicos, otro 32% se originó mediante tráfico web y el restante 23% mediante tráfico de red. Con esta realidad, la mejor forma de que una organización esté preparada para esta realidad es formando a su personal. Cada usuario en un puesto de trabaja marca la frontera entre la jungla de Internet y la red corporativa, por lo que cada usuario de cada organización se convierte casi sin quererlo en el "primer agente de aduana" de la frontera entre la organización y el resto del mundo.

Si esa persona no está entrenada y debidamente formada para detectar web maliciosas y correos con virus, y no conoce el uso de técnicas de ingeniería social para acceder a información privada, entonces la empresa podrá verse envuelta en serios problemas.

Por tanto, una de las mejores formas de prevenir y defender la empresa de un ciberataque es la formación del personal que lo compone. ¿Cómo se puede

acceder a esta formación? Existen planes de formación ideados por expertos en ciberseguridad que coinciden en estos puntos:

-Aprendizaje con ejemplos reales de infección de compañías y los efectos de dichos ciberataques en las mismas.
-Formación técnica específica sobre malwares, virus, *phising*y técnicas de ingeniería social.
-Módulos de capacitación para los empleados que incluyan una evaluación de los conocimientos adquiridos
-Seguimiento a través de una formación continua que mantenga a los empleados informados sobre nuevas amenazas.

Así, una empresa será mucho más segura si tiene una buena plantilla formada junto con el seguimiento de un procedimiento de trabajo detallado en un plan director de Ciberseguridad. Este plan director debe coordinar las medidas de defensa de la empresa (como puede ser el uso de Firewalls, IDS, antivirus y antimalware), activar protocolos de actuación ante un ciberataque y preservar una buena política de copias de seguridad y medidas de control.

En nuestra mano está convertir nuestras empresas en organizaciones más seguras. Por este motivo recomendamos productos como los de hardening de usuarios que ayudan a las empresas a estar más seguras.

Artículo realizado por Dolbuck Seguridad Informática