En el ámbito empresarial cuando hablamos de ciberseguridad no solo hacemos alusión a las medidas técnicas, tecnologías o procesos necesarios para garantizar la protección de la información. No podemos olvidar que el usuario es el eslabón más importante de la cadena de la seguridad, por lo que su acción o inacción serán fundamentales a la hora de corregir vulnerabilidades, protegerse ante ciberataques o evitar caer en las trampas de los ciberdelincuentes.

La seguridad de la información está en constante evolución, ya que los vectores de ciberataque son cada vez más sofisticados y complejos, haciendo un mayor uso de la ingeniería social para conseguir llegar a sus víctimas potenciales. Por este motivo, de cara a reducir riesgos y garantizar un mayor grado de protección, se hace necesario ir siempre un paso por delante.

Para conseguirlo, tendremos que ir más allá de la seguridad que proporcionan los elementos tecnológicos y confeccionar un sistema de defensa basado en las personas, conocido como ***firewall humano***. Se trata de un concepto del que ya os hemos hablado en alguna ocasión y que convierte al trabajador de una empresa en un importante mecanismo de defensa ante un ciberataque.

¿Qué es un cortafuegos humano?

Es aquel compromiso adquirido por un grupo de personas, en este caso de trabajadores de una entidad, para llevar a la práctica aquellas medidas, tanto preventivas como reactivas, que tengan como objetivo la implementación de ciberseguridad.

Dado que la evolución de medidas de protección tecnológicas cada vez protegen más y mejor nuestros sistemas de información, los ciberataques se están enfocando en buscar el error del usuario. Por esta razón, se suele decir que en la cadena de la ciberseguridad el usuario es uno de los eslabones más débiles, y por lo tanto, lo convierte en el eslabón más importante.

La cadena de la ciberseguridad será tan fuerte como su eslabón más débil.

Formación y concienciación

Si queremos contar con un verdadero firewall humano que fortalezca la cadena, tendremos que asegurarnos de que en todo momento nuestros empleados conocen, entienden y cumplen todas las normas y medidas de protección que se tienen implementadas en materia de ciberseguridad, advirtiéndoles de los riesgos asociados a una mala praxis, tanto de dispositivos como de soluciones que se encuentren dentro de su alcance. Para conseguirlo deberemos:

- Garantizar una correcta difusión de las políticas de seguridad, documentándolas, explicándolas minuciosamente y dejándolas al alcance de todo el personal de la empresa.
- Concretar un plan de formación que englobe los procedimientos y controles básicos, informando debidamente de las normas, leyes o contratos que rigen en la organización, dejando claras las medidas de protección asociadas al puesto de trabajo, qué aplicaciones están permitidas, cómo se deben tratar los datos personales, etc.
- Establecer programas de formación específicos para ciertos perfiles o empleados, ya sean técnicos de soporte, administradores de sistemas o nuevos empleados.
- Concretar periodos formativos. De esta forma, se pueden llevar a cabo acciones formativas que giren en torno a actualizaciones en materia de ciberseguridad para reforzar las debilidades detectadas o incidir en mensajes de mayor importancia.
- Exigir a las entidades externas con las que se tenga interactividad que sus políticas de ciberseguridad estén alineadas con las nuestras.
- Evaluar el aprendizaje obtenido que ayude a determinar el grado de concienciación alcanzado y las debilidades que habrá que reforzar.

La ingeniería social

Se trata de una de las técnicas más utilizadas a la hora de evitar las defensas tecnológicas de cualquier organización. Su principal objetivo es esquivarlas dirigiendo el foco de atención hacia el empleado. De este modo, el vector de ciberataque se basa en su habilidad para manipular, engañar e influir en las acciones o actuaciones del usuario final, en este caso del trabajador.

En función de la interacción del ciberdelincuente con la víctima, las técnicas de ingeniería social pueden ser:

- Pasivas: se basan en observar el comportamiento de la víctima.
- No presenciales: se basan en solicitudes de información a través de correos electrónicos, llamadas, suplantación de identidades, etc.
- Presenciales no agresivas: incluyen una vigilancia de la víctima, es decir, de su domicilio, analizando su entorno, ya sea el personal como el profesional, así como de sus amistades, compañeros, etc.
- Agresivas: se basan en la presión psicológica y la suplantación de identidad, normalmente del entorno cercano a la víctima.

Por lo tanto, hay que ser conscientes de que cualquier compañía, sin importar el tamaño o sector al que dedica su actividad, puede ser vulnerable. El ciberdelincuente puede lanzar un ciberataque sin romper las medidas de seguridad y conseguir mediante un engaño que un empleado inconscientemente proporcione información valiosa a través de un correo, mensaje de texto, llamada telefónica o incluso inicie o lance un ciberataque, ya sea ejecutando una archivo, haciendo clic en un enlace, etc.

Los ciberataques de ingeniería social podrían basarse en aspectos tecnológicos, como el spam, las ventanas emergentes en los navegadores, software malicioso, *phishing* o *pharming*, entre otros; o basándose en el aspecto humano, es decir, explotando las debilidades del comportamiento humano, aprovechándose de la voluntad de ayudar, del respeto a la autoridad, del temor a la pérdida de un servicio, etc.

En ambos casos, lo más importante para frenar este tipo de ciberataques es contar con un firewall humano robusto, basado en la formación y concienciación. Las últimas novedades del mercado tecnológico no servirán de mucho si mediante un simple correo electrónico un ciberdelincuente se hace con información confidencial de nuestra empresa.

Existe una gran cantidad de técnicas mediante las cuales los ciberdelincuentes acceden a sus objetivos. Algunas requieren de tecnología pero otras basan su acción en la manipulación humana. Minimizar o mitigar estos riesgos dependerá del compromiso que los trabajadores de una entidad tengan con la ciberseguridad. Asegúrate de que todos conocen los procedimientos y cuenten con una verdadera cultura de seguridad. De esta manera tendrás configurado y listo tu firewall humano.