HORNETSECURITY

EMPLOYEE SECURITY INDEX

WHITEPAPER

Ingeniería social: el usuario como puerta de entrada

La continua actualización de las medidas técnicas de protección en el ámbito de la seguridad informática va de la mano de un repunte de los ataques ligados a la ingeniería social en todo el mundo: mientras que, en 2013, un 17% de todos los ciberataques tenían un componente de ingeniería social, hoy en día ya la práctica mayoría de todos los ataques se asocian a la ingeniería social. La expansión masiva del software malicioso Emotet y sus sucesores muestra la dimensión y la calidad que pueden alcanzar estos ataques. Emotet lee los contactos y el contenido del correo electrónico de las bandejas de entrada en los sistemas infectados, y utiliza esta información para seguir expandiéndose. Estos mensajes de *spear phishing* apenas suelen ser apenas reconocibles para los no expertos.

La concienciación en seguridad («Security Awareness») refuerza el «cortafuegos humano»

Por eso, en ningún diseño de seguridad de la información puede faltar el factor humano: la palabra clave es «Security Awareness». El «Security Awareness» indica hasta qué punto los empleados son conscientes de la importancia de la seguridad de la información en su empresa y el alcance de su propia responsabilidad en esta materia, sobre todo, describe en qué medida la aplican.

Existen diferentes medidas que se pueden aplicar para aumentar la Security Awareness. Es importante no considerar al usuario como un riesgo sino, más bien, como un elemento esencial de la solución en seguridad informática: «tú eres el cortafuegos de tu empresa». Por eso, se debe integrar a los empleados, no sobrecargarlos y, sobre todo, no atemorizarlos.

Sin embargo, la planificación de medidas para aumentar la Security Awareness encierra numerosos retos:

- ¿Cómo se puede asegurar que las medidas en materia de Security Awareness son eficaces y sostenibles?
- ¿Es posible obtener un retorno de la inversión? ¿Merece la pena la inversión?
- ¿Existe un indicador o comparativa con organizaciones de sectores similares?
- ¿Pueden recibir los empleados de una organización una formación a medida en lugar de un único método para todos?

Con el Employee Security Index, o ESI®, la conducta de seguridad de los empleados resulta cuantificable de una forma realista, estandarizada y replicable. En este Libro Blanco se detalla el proceso de cálculo y se presenta un índice de referencia extraído de más de 60 empresas europeas.

La clasificación de los ataques como base para un método de medición estandarizado

Para que la Security Awareness se pueda medir, es indispensable realizar una simulación realista de los ataques de *spear phishing*. Además, cada ataque debería poder compararse con los demás. Solo a través de una medición en un periodo más largo de tiempo se puede aportar información sobre la evolución de la Security Awareness.

Por eso clasificamos en diferentes categorías los escenarios de phishing subyacentes. Al hacerlo, resulta determinante el tiempo que deberá invertir un atacante en preparar y llevar a cabo un escenario de ataque. Este tiempo se compone, por ejemplo, de la obtención de información OSINT (inteligencia de fuentes abiertas), la preparación técnica, el copiado de los diseños de páginas web y el hecho de contar con una determinada infraestructura. Así, los escenarios de phishing se pueden clasificar en siete categorías (llamadas «niveles»), cada una de las cuales requiere diferentes tiempos de preparación.

Nivel	Ejemplo	Tiempo de preparación
1	Típico mensaje masivo de phishing, como puede ser el de confirmación de compra de un conocido portal de e-commerce	aprox. 15 minutos
2	Supuesto mensaje de correo del o la gerente (fraude del CEO)	aprox. 1 hora
3	Mensaje de correo de *spear phishing*, que incluye información pública sobre la empresa (extraída, por ejemplo, de portales de valoración de empleadores)	aprox. 2 horas
4	Mensaje de correo de *spear phishing* que hace referencia al departamento y al cargo del destinatario, emails de compañeros o superiores directos	aprox. 4 horas
5	Mensaje de correo que suplanta la identidad de un partner que no ha activado una protección contra el *spoofing* de correo electrónico o al que le han hackeado una cuenta	aprox. 6 horas
6	Un partner o compañero de trabajo ha sufrido un hackeo: mensaje de correo de un contacto personal en el que se responde a una conversación de correo previa.	aprox. 12 horas
7	Mensaje de correo de *spear phishing* relacionado con temas en los que ya está trabajando el propio destinatario (la actualización del estado de un proyecto en marcha en el que participa el destinatario, por ejemplo).	Más de 20 horas

Tabla: resumen de los tiempos de preparación

Índice de Security Awareness: el ESI®, o Employee Security Index

Para medir el grado de concienciación de un grupo de estudio, cada empleado participante se convierte en el objetivo de determinados escenarios de ataque en diferentes categorías, seleccionados aleatoriamente. A continuación, se mide la «tasa de éxito» (desde el punto de vista del atacante) en el grupo de estudio.

Esperar una «tasa de éxito» cero como objetivo a cumplir es irreal, ya que las personas cometen errores. Por eso nuestra definición de grupo de estudio «ejemplar» se sitúa en un punto medio entre la seguridad y la viabilidad. Dependiendo del tiempo de preparación que debe dedicar un atacante, definimos unos valores de tolerancia dentro de los cuales podemos seguir considerando el comportamiento de los empleados como «ejemplar» en lo que respecta a la seguridad. Estos valores están entre un 1,1 y un 6,2 % en las categorías 1 a 7.

Un grupo de estudio que muestre exactamente estas tasas de éxito obtiene un valor ESI® de 90. Si se da un comportamiento sensible con el doble de frecuencia, por ejemplo, al hacer clic en el enlace dañino de un mensaje de correo de phishing, el grupo obtiene un ESI® de 80; si la frecuencia es del triple, entonces el valor es de solo 70. Los valores situados por debajo de 70 se clasifican como sensibles (véase la figura 1).

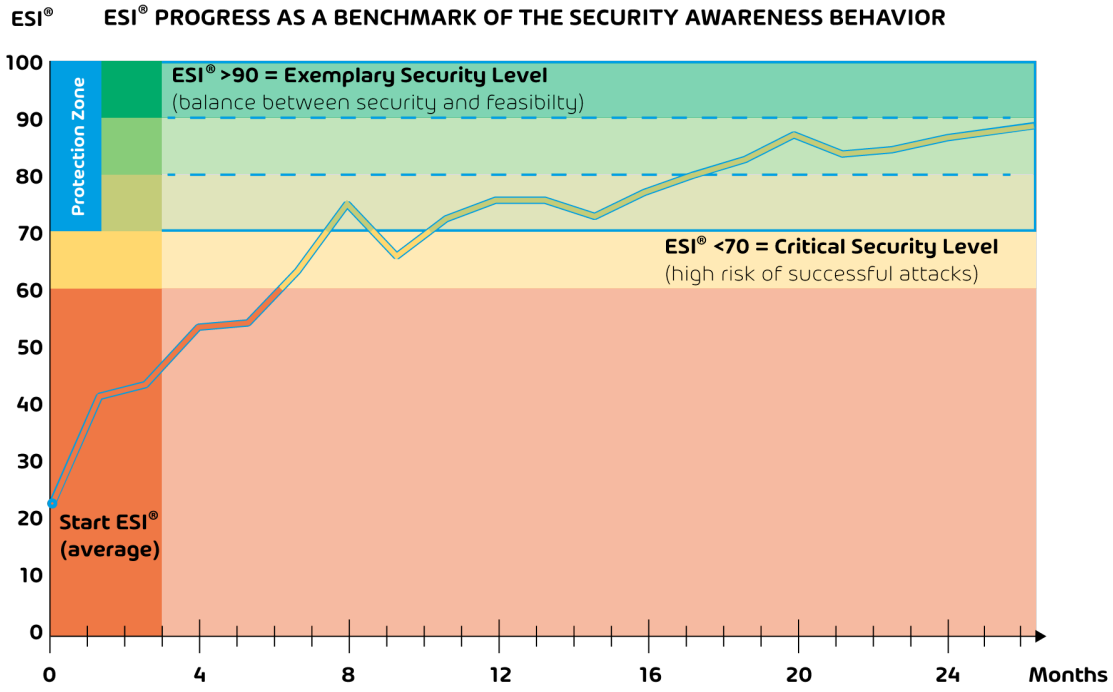

Figura 1: Ejemplo de la evolución temporal del desarrollo del ESI® como referencia de la cultura de seguridad

El cálculo del ESI® en empresas europeas indica que la Security Awareness es deficiente, pero las mejoras significativas a través de la formación son apreciables.

El Employee Security Index se calcula desde mediados de 2018 como parte de las simulaciones de phishing en empresas e instituciones con operaciones internacionales. En concreto, se mide la tasa de clics en enlaces y archivos adjuntos. Como ejemplo de ataques simulados podemos citar los siguientes: un supuesto aviso de que el almacenamiento de la bandeja de entrada está lleno (categoría 1), el mensaje de correo de un compañero de trabajo tomado al azar que envía un enlace a un GIF gracioso (categoría 2) o la consulta realizada por un jefe de departamento sobre una factura que se adjunta (categoría 4). De este modo, la simulación de phishing se ha llevado a cabo de la forma más realista posible: todos los participantes recibieron ataques individuales de *spear phishing* en momentos aleatorios.

La valoración obtenida de más de 1,7 millones de ataques simulados de phishing arroja una esclarecedora imagen sobre el comportamiento de los empleados en cuanto a la seguridad en empresas de todos los sectores y tamaños, como queda reflejado en la figura 2 para un periodo de doce meses.

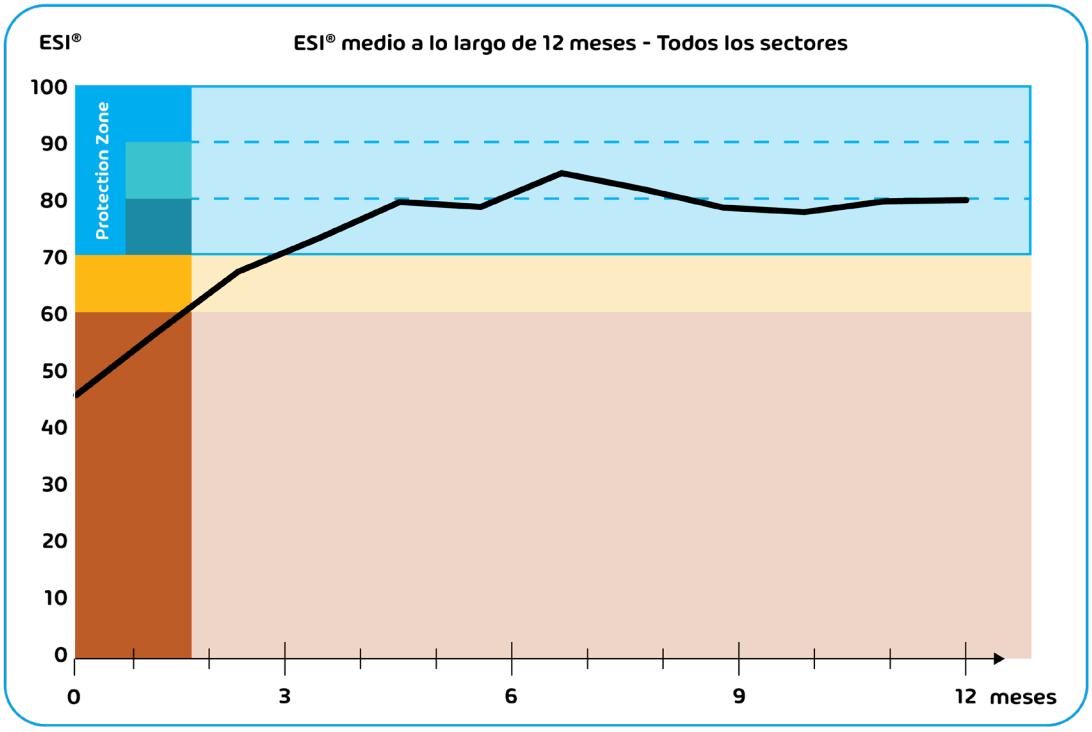

Figura 2: cálculo del ESI® medio a partir de la simulación de phishing

Es necesaria una formación continua en concienciación

El desarrollo medio del ESI® indica claramente en los primeros doce meses la razón por la cual es necesaria una formación continua para mantener un buen nivel de seguridad incluso en periodos prolongados de tiempo. Mientras que al principio la curva ESI® aumenta de forma continua y enseguida alcanza un nivel aceptable de seguridad, a medida que los escenarios de *spear phishing* se vuelven más ingeniosos es evidente que resulta más difícil mantener el nivel, sobre todo si se están incorporando constantemente nuevos empleados o si hay grupos o empleados concretos que dejan temporalmente la formación. Esto se aprecia en la figura 3.

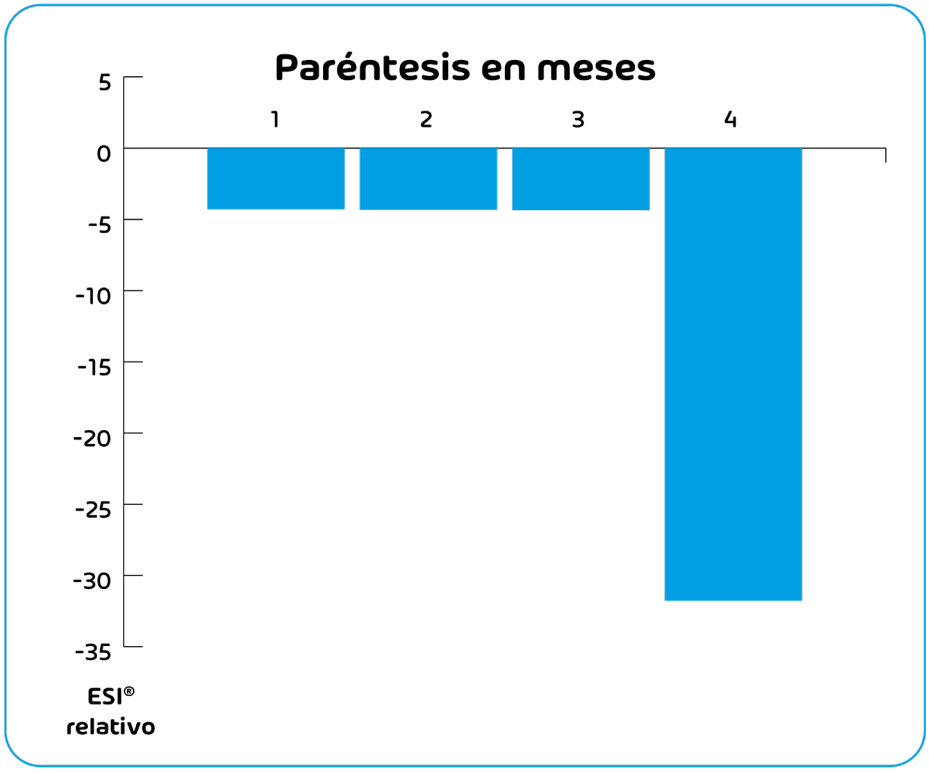

Figura 3: Caída del ESI® tras un paréntesis en la formación

Se requiere una formación continua de sensibilización

La concienciación es un músculo que debe ser entrenado con regularidad; de lo contrario, se relaja. Cuando hay trabajadores o grupos que interrumpen la formación para retomarla más adelante, se observa una clara caída en el comportamiento de seguridad: sin formación, los trabajadores se muestran más descuidados durante estas pausas y olvidan contenidos importantes. En esta gráfica, la caída del ESI® muestra este efecto demoledor: ya en el primer mes de pausa en la formación, el ESI® cae 5 puntos, situándose a menudo por debajo del nivel de seguridad que se pretende lograr. A los 4 meses, el ESI® ya desciende en más de 30 puntos (y se vuelve prácticamente a la misma posición en la que se estaba al inicio de la formación).

Un instrumento de control como base para determinar más medidas de concienciación en materia de seguridad

El ESI® representa en este sentido un instrumento de control con el que se puede supervisar de forma continua la Security Awareness de las empresas. Se puede comprobar la efectividad de las medidas individuales de formación y diagnosticar necesidades más específicas. Gracias a un indicador concreto se facilita la comunicación tanto con la gerencia como con el personal: el análisis cuantitativo de la Security Awareness ofrece una comparación directa con otras empresas de sectores similares, pudiendo utilizarse como fundamento a la hora de decidir sobre otras inversiones.

Formar a los empleados: un proceso totalmente automático con el Security Awareness Service

La sensibilización de los empleados en Security Awareness es esencial para proteger eficazmente a una empresa de ciberataques, ya que las medidas técnicas de seguridad por sí solas no son suficientes si los atacantes saben cómo aprovechar las vulnerabilidades humanas.

No obstante, esta tarea supone un reto para muchos responsables en seguridad informática, ya que una formación sostenida para los empleados puede implicar mucho tiempo y recursos. Nuestro Security Awareness Service le permite ahorrarse la mayor parte de este trabajo.

Nuestro Security Awareness Service forma a sus empleados basándose en indicadores ESI®, según las necesidades concretas y de modo totalmente automatizado para lograr una sensibilización sostenible y eficiente. El programa continuo de formación incluye diversos métodos para llegar de manera eficaz a los trabajadores: desde la simulación de phishing, pasando por la formación en línea y vídeos breves, hasta material sobre concienciación. El resultado es una cultura proactiva de la seguridad y unos empleados formados que conocen y tienen en cuenta su responsabilidad con la empresa. El Awareness Engine supone el núcleo tecnológico de nuestro Security Awareness Service y ofrece la medida idónea de formación para cada caso: cada participante recibe tanta formación como necesita y en la menor medida posible.