Kaspersky Security Awareness

El factor humano es uno de los principales factores a tener en cuenta en la ciberseguridad corporativa

Si bien en los últimos años la mayoría de las organizaciones ha instalado firewalls y filtros de phishing avanzados e implementado herramientas especializadas para mitigar las ciberamenazas, los cibercriminales han convertido a los empleados en su habitual punto de entrada a los sistemas de IT. Para estos delincuentes, aprovechar las lagunas de conocimientos de los usuarios supone la forma más fácil de penetrar en la infraestructura de IT corporativa.

Según la encuesta elaborada por Kaspersky y B2B International*, el **52 %** de las empresas admite que los empleados son el mayor punto débil en materia de seguridad de IT, debido a falta de conocimientos o a acciones descuidadas que acaban poniendo en peligro su estrategia de seguridad de IT.

Entre los aspectos que más preocupan a las organizaciones destacan que los empleados compartan datos inapropiados mediante sus dispositivos móviles (47 %), la pérdida física de dispositivos móviles y los riesgos que esto entraña para la empresa (46 %), y el uso inapropiado de los recursos de IT por parte de los empleados (44 %).

Si analizamos en más detalle estos datos, la preocupación por un uso inapropiado de los recursos de IT por parte de los empleados varía considerablemente según el tamaño de la organización. Por ejemplo, a las empresas más pequeñas (de 1 a 49 empleados) les preocupa más el riesgo de estas amenazas que a aquellas que tienen más de 1000 empleados. Esta diferencia podría deberse a distintos factores, como el hecho de que las grandes empresas puedan tener en marcha políticas más estrictas y forman más concienzudamente a sus empleados sobre prácticas ciberseguras.

Los errores humanos son la principal causa de los ciberincidentes

El estudio sobre inteligencia de ciberseguridad Cyber Security Intelligence Index de IBM ha revelado que más del 90 % de todos los incidentes de seguridad implica algún tipo de error humano: desde seguir enlaces de estafas de phishing hasta visitar sitios web maliciosos, lo que permite a los virus actuar y puede acarrear otras amenazas persistentes avanzadas.

La encuesta de 2017 realizada por Kaspersky Lab y B2B International* respalda estas conclusiones. Según este informe, un aspecto común del factor humano, el uso inapropiado de los recursos de IT por parte de los empleados, ha contribuido a que los ataques experimentasen un aumento del 39 % en organizaciones de todo el mundo en un periodo de 12 meses.

Impacto financiero medio provocado por acciones inapropiadas de empleados descuidados o desinformados[1]

Para pymes

- Intercambio inapropiado de datos: 77 056 EUR
- Pérdida física de dispositivos móviles que exponen a la organización a riesgos: 86 700 EUR
- Pérdida física de dispositivos o medios que contienen datos: 70 900 EUR
- Uso inapropiado que los empleados hacen de los recursos de IT 60 000 EUR

Para grandes empresas

- Incidentes por dispositivos conectados ajenos a IT: 1 401 000 EUR
- Pérdida física de dispositivos o medios que contienen datos: 963 000 EUR
- Uso inapropiado que los empleados hacen de los recursos de IT: 509 000 EUR
- Intercambio inapropiado de datos mediante dispositivos móviles: 406 000 EUR

Robo de datos en números[2]**:**

- El 61 % de las víctimas de robo de datos del informe de 2017 son empresas de menos de 1000 empleados.
- En el 81 % de las infracciones de pirateo se utilizaron contraseñas robadas o contraseñas débiles, fáciles de adivinar.
- El 43 % de las infracciones son ataques sociales.
- El 66 % del malware se instala mediante archivos adjuntos de correo electrónico que resultan ser maliciosos.

1. "Global IT Security Risks Survey 2017". Blog de Kaspersky Lab y B2B International
2. "2017 Data Breach Investigations Report" Verizon

El aumento en el número de incidentes cibernéticos causados por errores humanos es especialmente notable en las empresas muy pequeñas. En un solo año, el porcentaje de estas organizaciones que ha sufrido ataques relacionados con los empleados ha aumentado de un 25 % a un 32 %.
Lo más preocupante es que prácticamente la mitad de todas las empresas (entre el 44 y el 48 %) no se sienten bien protegidas ante las amenazas derivadas del desconocimiento, la ingenuidad o el fraude de sus propios empleados.

Como segunda causa de todos los incidentes, las organizaciones también identificaron la falta de información o cuidado por parte de sus empleados: el 46 % de los encuestados mencionó este motivo como el principal causante de los incidentes sufridos.
Es cierto que los empleados constituyen el principal acceso a la organización para los atacantes. Pero contar con un personal bien formado e informado, que ponga en práctica medidas efectivas de cultura cibernética y esté al tanto de las novedades del mundo cibernético, también puede convertirse en su primera línea de defensa.

*"Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within", junio de 2017

Concienciación eficaz en materia de seguridad

Formar al personal resulta esencial para fomentar la concienciación entre los empleados y motivarles a prestar atención a las ciberamenazas y a las tácticas defensivas, incluso cuando estas tareas no se perciben como parte de las responsabilidades del puesto de trabajo.

Por desgracia, muchos programas formativos de concienciación son poco eficaces. En muchos casos, se aplican políticas de seguridad, se proporciona la información más reciente sobre los tipos de malware existente y las medidas de protección, pero no se observan los resultados esperados tras la formación. ¿Cuál es el problema?
La formación de concienciación en materia de seguridad suele asociarse con demasiada frecuencia a sesiones obligatorias de medio día de duración, en las que los trabajadores tienen que permanecer enfrente de la pantalla, fingiendo que prestan atención a una presentación de PowerPoint mientras usan el teléfono a escondidas. Dicha formación es, obviamente, una pérdida de tiempo, y los empleados siguen actuando igual que antes de recibirla.
Las formaciones de concienciación sobre seguridad también han demostrado ser poco efectivas si se abruma a los empleados con demasiadas instrucciones sobre lo que deberían o no deberían hacer. Es imposible asimilar tanta información, y esta sobrecarga puede generar un sentimiento de pesimismo.

Un programa efectivo de concienciación sobre seguridad debería abarcar cuatro aspectos clave:

Definición de los objetivos formativos y motivo del programa
- Establecimiento de objetivos que puedan medirse con respecto a parámetros de referencia
- Búsqueda de un equilibrio entre los niveles esperados de competencias de seguridad necesarios para cada grupo de empleados y el tiempo de aprendizaje total requerido para que los empleados lleguen a dichos niveles

Garantía de que todos los empleados reciben formación al nivel esperado como mínimo
- Uso de herramientas de gestión del aprendizaje automatizadas para garantizar que todos los empleados lleguen al nivel de conocimientos de seguridad apropiado según su perfil de riesgo
- Consolidación de las habilidades adquiridas para asegurar su retención
- Formación individualizada, que permita a cada uno avanzar a su ritmo

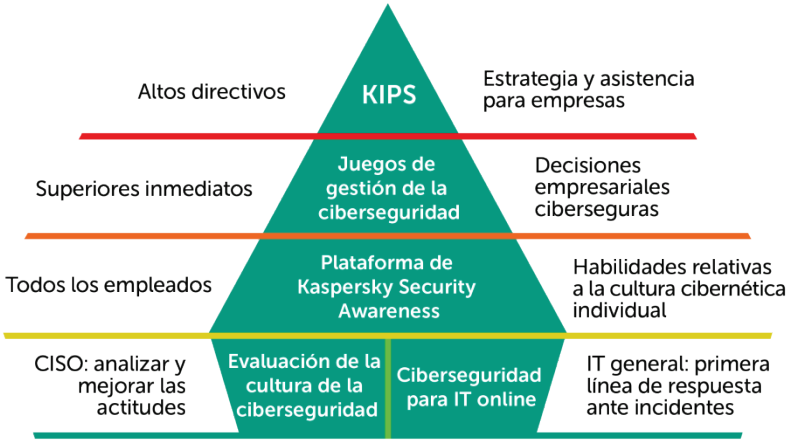
Control del progreso con análisis e informes procesables
- Seguimiento de datos, tendencias y previsiones en directo
- Uso de previsiones en tiempo real para lograr los objetivos de formación anuales
- Resolución de las incidencias antes de que se conviertan en problemas (al saber qué áreas de la organización requieren más atención y respuesta)
- Comparación de resultados provisionales con parámetros de referencia

Garantía de valoración de la formación y, por tanto, de asimilación
- Participación de los empleados en la formación mediante técnicas de competición y ludificación
- Garantía de que la formación sea relevante para las tareas cotidianas de los empleados
- Oportunidad de comparar los resultados con los de otros compañeros
- Prevención de la sobrecarga informativa

Entender lo que hay detrás de cada formación ayuda a desarrollar un programa educativo eficaz.
En Kaspersky Lab ofrecemos una familia de productos de formación online que utilizan las técnicas de aprendizaje más avanzadas y abordan todos los niveles de la estructura empresarial. Nuestros programas no solo ofrecen conocimientos: ayudan a establecer nuevos patrones de comportamiento, lo que es mucho más importante y constituye el objetivo real de cualquier formación de concienciación.

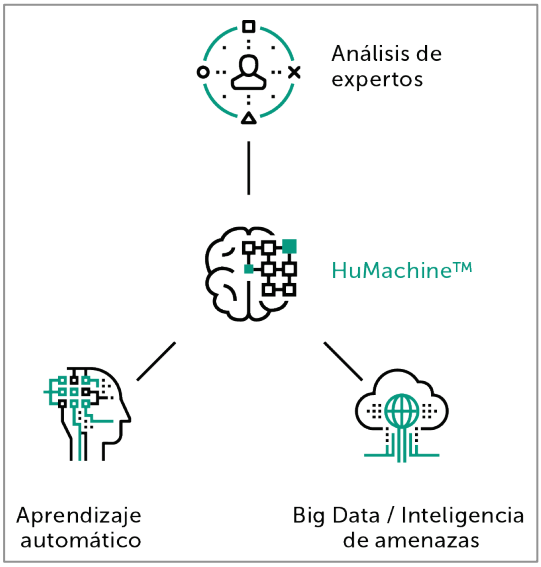
El enfoque integral que Kaspersky Lab adopta se basa en modernas técnicas de aprendizaje donde se combinan la gamificación, los ejercicios prácticos, las dinámicas de grupo y el refuerzo. De todas estas técnicas, la gamificación resulta la más interesante, ya que redefine las actitudes de los participantes y desarrolla nuevos patrones de comportamiento, lo que permite crear sólidos lazos emocionales y, por tanto, fomentar la motivación a la hora de aprender

Programas de formación Kaspersky Security Awareness



Este enfoque cuenta con resultados demostrados:

- Reducción de hasta el 90 % en el número de incidentes
- Disminución de hasta el 50 % del impacto financiero de los incidentes
- Increíble tasa de recomendación del programa del 86 % entre los participantes



Kaspersky Lab

Enterprise Cybersecurity: www.kaspersky.com/enterprise
Noticias de ciberamenazas: www.securelist.com
Noticias de seguridad de IT: business.kaspersky.com

#truecybersecurity
#HuMachine

www.kaspersky.es