ICE
ISRAEL
CYBERSECURITY
ENTERPRISE

Nuestra **única prioridad** es la ciberseguridad de nuestros clientes

10 mejores prácticas para un programa eficaz de simulación de “phishing”

Manual de simulación de phishing

CYBEREADY

www.ice.lat

ICE
ISRAEL CYBERSECURITY ENTERPRISE

CYBERREADY

¿Se pregunta cómo proteger eficazmente a su organización contra los intentos de phishing?

Siga estas prácticas recomendadas para transformar el comportamiento de sus empleados y aumentar la resiliencia de la organización.

Usted es muy consciente de los riesgos a los que se enfrenta como profesional de la seguridad; después de todo, son numerosos, evolucionan constantemente y están siempre presentes. Y gran parte de los resultados que puede obtener dependen de personas que dedican poco tiempo a pensar en la seguridad.

Ojalá que la seguridad fuera una cuestión prioritaria para todo su personal. Como probablemente no lo sea, es crucial que pueda planear, poner en marcha y evaluar un programa de capacitación sobre conciencia en materia de ciberseguridad que verdaderamente transforme el comportamiento de los empleados. Sin embargo, para que este esfuerzo tenga éxito, implicará mucho más que simplemente enviar correos electrónicos a los empleados.

Para obtener resultados óptimos a largo plazo, las compañías deben seguir una metodología científica que implemente las siguientes mejores prácticas:

Capacitación total de la fuerza laboral

Las investigaciones muestran que los intentos ad hoc y dispersos para capacitar a subgrupos del personal son en gran medida ineficaces. Para reforzar las defensas internas contra las sofisticadas amenazas de ‘phishing’, debe capacitar al 100% de sus empleados cada mes. Esto se hace más complicado a medida que los equipos crecen y se extienden por varias ubicaciones. Sin embargo, optar por algo menos que la capacitación total de la fuerza laboral conduce a resultados fragmentados, dejando "vacíos" de seguridad en forma de empleados ingenuos. La peor parte: una cobertura incompleta de la fuerza laboral significa no conocer la conciencia actual de algunos empleados sobre las amenazas, lo que potencialmente hace que se pasen por alto los eslabones más débiles que ponen a la organización en mayor riesgo. Para cuando los ‘hackers’ los aprovechen, usted estará llevando a cabo un triaje de emergencia interno y externo con la dirección de la compañía, recursos humanos y el personal de relaciones públicas.

Aprendizaje justo a tiempo

Existe una ventana de tiempo limitada en la que las lecciones derivadas de la capacitación tendrán el mayor impacto a largo plazo en los empleados. Este es el "momento de oro" - la instancia en la que proporcionar un contenido oportuno, atractivo y eficaz puede causar una impresión duradera, en contraste con tener que imponer sesiones adicionales de capacitación que a menudo se perciben como aleatorias, irrelevantes y menos memorables - por no hablar de que son más difíciles de imponer. La clave está en asociar los riesgos a comportamientos específicos de los empleados. El personal que experimenta el aprendizaje "justo a tiempo" tiene más probabilidades de retener el conocimiento crítico y la conciencia de los factores de riesgo, y es más capaz de responder de manera adecuada en futuros escenarios de ataque. En esencia, las compañías deben asegurarse de que cualquier empleado que sea embaucado por una simulación participe inmediatamente en una sesión de formación que cubra los errores que ha cometido.

Ciclo continuo

La capacitación no debe llegar en oleadas predecibles. Mediante la implementación de un programa continuo, su personal podría ser sorprendido con la guardia baja y tener más oportunidades de aprender. Generar la expectativa de que una amenaza podría presentarse en cualquier momento también anima a los empleados a permanecer alerta entre una campaña de capacitación y otra. Aquellos que sólo están expuestos a simulaciones ocasionales son más propensos a cometer errores fácilmente evitables, ya que los escenarios de ataque cambian rápidamente. Un ciclo continuo garantiza que todo el personal nuevo será debidamente integrado, y refuerza el hecho de que la seguridad es una cuestión de importancia 24 horas al día, 7 días a la semana, y no sólo es marcar una casilla de cumplimiento para satisfacer los requisitos mínimos.

Nivel de dificultad ajustado

En algún momento, todo el mundo domina los fundamentos de la identificación de amenazas. Sin embargo, dado que los actores maliciosos no se detendrán ahí, su capacitación tampoco debería hacerlo. Es importante comenzar con un nivel de dificultad bajo e ir subiéndolo continuamente, ajustando los niveles de dificultad y los contextos de las simulaciones con el fin de sustentar un aprendizaje más sólido para los empleados. Dicho esto, pronosticar la dificultad real es un proceso complejo; requiere de un monitoreo diario del desempeño de la campaña para asegurar que cualquier suposición con respecto a grupos específicos fue acertada. También se recomienda que su equipo de seguridad se mantenga al tanto de la evolución de las tendencias globales de ‘phishing’, ya que varios estilos y escenarios de ataque se harán más populares en algunas zonas geográficas o idiomas que en otros.

Intervalos oportunos de capacitación

Aunque el elemento sorpresa es importante, llevar a cabo una capacitación de seguridad totalmente aleatoria o esporádica es contraproducente. Las compañías más seguras se cercioran de que las campañas de 'phishing' se produzcan en intervalos de tiempo programados. Estos pueden solaparse entre sí, pero pueden establecerse una o dos veces al mes, cada dos meses o más. Un calendario fijo permite a los CISO y a sus equipos establecer una base general sólida para el desempeño global de los empleados. La comprensión obtenida a partir de datos cuantitativos relativos al "punto de partida" o a la respuesta típica ante amenazas de los miembros del personal, le permite a usted identificar sus mayores áreas problemáticas y determinar cómo mitigarlas. Nota: el desempeño individual de los empleados entra en juego sólo después de que usted haya establecido intervalos y un punto de referencia.

Reportes detallados de BI

Todos los caminos conducen a sus datos de capacitación. Pero los reportes no deben limitarse a indicar el estado actual de la seguridad de su compañía o a precisar los puntos débiles; deben medir y mostrar en tiempo real los indicadores clave de desempeño (KPI) y la inteligencia de negocios que se desglosa por país, departamento, equipo u otros niveles, todo ello sin violar la privacidad individual de los empleados. Los reportes deben contener gráficos claros y concisos e información resumida que transmita cambios sustanciales. Si se asegura de que las principales partes interesadas reciban reportes semanales, resúmenes de campañas e informes trimestrales de operaciones con datos procesables, se les mantendrá al tanto de los progresos en curso y se les ofrecerá una visión del impacto a largo plazo de su programa de capacitación. Usted también eliminará el trabajo administrativo innecesario para demostrar la eficacia de sus esfuerzos; en lugar de ello, su equipo podrá atender asuntos de seguridad más urgentes.

Capacitación basada en datos

Los profesionales de la seguridad saben que los empleados responden de forma diferente a diversos vectores de ataque. Para los conocidos como "clickers seriales", una reacción instintiva para descargar, hacer clic o abrir un archivo adjunto a menudo puede ponerlos (a ellos y a sus organizaciones) en peligro. Identificar y mantener una lista actualizada de los “clickers seriales” requiere de un monitoreo consistente del desempeño de todos los empleados. Pero no son el único grupo que usted debe examinar; las nuevas contrataciones, el liderazgo ejecutivo y los empleados veteranos responden de manera diferente a las amenazas potenciales, por lo que es posible que desee analizar los datos para comprender mejor cómo se comportan estos grupos. Después, su equipo debe ser capaz de crear campañas especialmente diseñadas para que estos grupos diferentes o potencialmente problemáticos adopten un enfoque más perspicaz de la gestión del correo electrónico. El "plan de tratamiento" que elabore debe incluir una frecuencia ajustada, recordatorios oportunos, simulaciones personalizadas y contenidos de capacitación que ayuden a reformar a los grupos especialmente susceptibles. Hacer todo esto es crucial, pero debe hacerse con el máximo respeto a la privacidad de los empleados.

Contenido adaptable

Una vez que haya colocado a los empleados en grupos segmentados, es hora de que la capacitación se vuelva adaptable. El nivel de dificultad del escenario es, por supuesto, sólo un parámetro. Determinar las futuras campañas de ataque basándose en el comportamiento individual es un factor crítico, al igual que adaptar el contenido para abordar específicamente los retos de un escenario determinado. Esto podría implicar solicitudes de contraseñas o datos, mensajes de remitentes o fuentes aparentemente legítimos, o contenido realista hecho a la medida del departamento o función de un empleado. El material que se adapta tanto a las respuestas individuales de los empleados como a determinados vectores de ataque sirve para afinar aún más las defensas de los empleados, convirtiendo al elemento humano en una ventaja para su compañía.

Frecuencia ajustable

Es probable que sus usuarios más avispados no se dejen embaucar dos veces por la misma simulación. Pero los "clickers seriales" son un caso aparte. Por lo tanto, el ritmo de sus campañas debe ser dinámico y personal, reflejando un nivel calculado de riesgo para los empleados a lo largo de la curva de aprendizaje con base en los datos que ha recopilado. Idealmente, usted necesitará crear frecuencias de campaña que se adapten a grupos de empleados hasta que se hayan ajustado a un determinado umbral de escenario de capacitación. Esto puede implicar, por ejemplo, que aquellos que se encuentren en un grupo de mayor riesgo recibirán inicialmente dos correos electrónicos de capacitación específicos por campaña, lo que les familiarizará aún más con el contenido de la capacitación y fomentará una respuesta diferente.

Contexto globalizado

Si usted forma parte de una compañía global cuyo idioma corporativo es el inglés, debería considerar el uso de contenidos multilingües que incluyan las lenguas maternas de sus empleados, ya que esto mejorará drásticamente la retención de su aprendizaje. De manera especial, en entornos empresariales multinacionales, es importante adaptar el material de capacitación en seguridad a las culturas en las que viven sus empleados. Dependiendo de la ubicación de su compañía, existen diversas implicaciones legales en relación con las normas de cumplimiento para el correo electrónico. Y al citar referencias locales en las simulaciones de capacitación, como fiestas nacionales, medios de noticias destacados, plataformas de medios sociales populares y ventas de temporada, usted aumentará las probabilidades de que sus simulaciones de correo electrónico sean creíbles, reforzando al mismo tiempo la conciencia de los empleados sobre ataques sigilosos y altamente realistas.

La planeación, la gestión y el análisis de una campaña de seguridad que incorpore las mejores prácticas mencionadas anteriormente proporcionará a las compañías resultados concretos. Pocas organizaciones que utilicen soluciones estándar son capaces de conseguirlo. El reto consiste en hacerlo manualmente, ya que el tiempo del personal suele ser muy valioso y la mayoría de los equipos de seguridad de las empresas carecen de los conocimientos especializados idóneos en todas estas categorías.

Ya sea debido a limitaciones internas de recursos o de tecnología, el resultado es el mismo: empleados con una capacitación inadecuada que se frustran con los escenarios elementales con los que se encuentran habitualmente. Esperar que los administradores de proyectos u otros miembros del equipo sin capacitación en ciencias cognitivas tomen decisiones y lleven a cabo acciones que ejecuten adecuadamente tales campañas es poco realista y está plagado de complicaciones, especialmente en el contexto de grandes empresas multinacionales.

Una plataforma impulsada por aprendizaje automático como CybeReady puede conseguirlo con eficacia. La solución ofrece a los equipos de seguridad un conjunto de sugerencias basadas en datos y reportes de BI (inteligencia de negocios) que utilizan las mejores prácticas de la industria. Esto se consigue por una fracción del costo de la creación y el análisis de simulaciones internas, ya que intentar ofrecer dicho contenido manualmente requiere una inversión de tiempo significativa.

La satisfacción de los empleados también aumenta con la capacitación en seguridad, ya que las simulaciones y su contenido de capacitación resultante se consideran relevantes y que valen la pena, en lugar de ser fortuitos, fuera de contexto o mal diseñados.
Y al introducir ataques más desafiantes basados en el desempeño anterior de los empleados, usted evitará que los intentos complejos de los hackers engañen a su personal, lo que reforzará aún más la relevancia duradera de su programa de seguridad. Y lo más importante: la plataforma correcta puede ayudar a las compañías a transformar el comportamiento de los empleados frente a posibles ataques por correo electrónico a largo plazo, lo que representa una ventaja competitiva significativa en cualquier industria que dependa en gran medida de la comunicación digital.

+52 (55) 1710 8373 | info@ice.lat | www.ice.lat
CDMX, México