INFORME ESI® BENCHMARK

EDICIÓN 2023

UNA EVALUACIÓN DE MÁS DE 1,7 MILLONES DE ATAQUES DE **SPEAR PHISHING SIMULADOS A EMPLEADOS**

EMPLOYEE SECURITY INDEX

HORNETSECURITY

INFORME ESI® BENCHMARK
EDITION 2023

Capítulo 1: Resumen ejecutivo

Phishing sin final a la vista: la cantidad de intentos de fraude llevados a cabo con mensajes de correo falsos no deja de batir cifras récord. Es cada vez más frecuente que los atacantes que emplean el phishing apunten a las empresas, ya que es ahí de donde más dinero pueden obtener. Estos atacantes envían mensajes de correo electrónico aparentemente confiables a los empleados con el fin de robar información sensible, descifrar datos o, en el peor de los casos, paralizar toda la actividad empresarial.

Con este Informe ESI® Benchmark queremos informarte del creciente peligro del phishing para tu empresa, así como de las opciones eficaces de defensa que existen. Nos centramos en el Security Awareness Training («formación en concienciación en seguridad») de Hornetsecurity, con el que puedes capacitar a tus empleados en un comportamiento de seguridad y establecer una cultura de seguridad informática perdurable. Su pilar fundamental es el Employee Security Index (ESI®), un método patentado que ofrece un índice para medir y supervisar la concienciación en seguridad.

Nuestra referencia actual, el índice ESI®, muestra cómo funciona exactamente. El estudio, en el que hemos analizado unos 1,8 millones de ataques simulados de spear phishing a trabajadores de empresas de todos los tamaños y sectores, aporta transparencia y proporciona importantes recomendaciones para optimizar la concienciación en seguridad de los empleados.

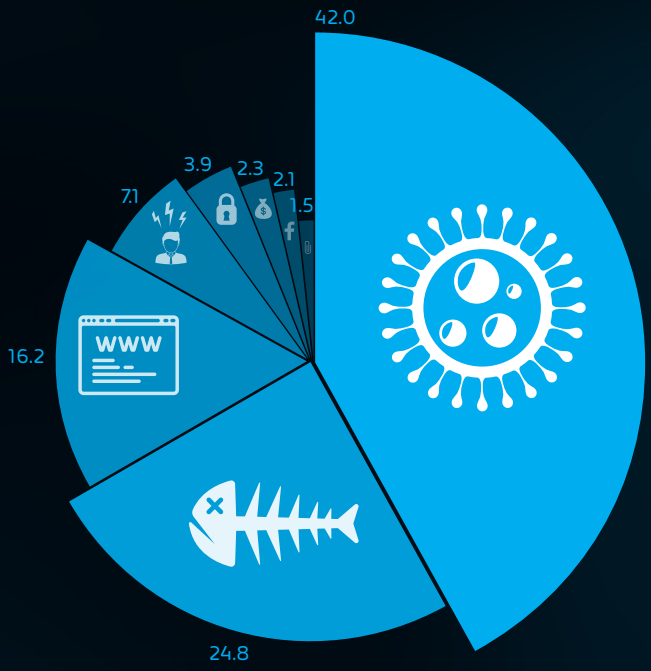
Como conclusión más destacable, cabe señalar que las empresas de todos los sectores alcanzan de promedio un nivel aceptable de seguridad (lo que se corresponde con un ESI de 70 como mínimo) tras tres meses de Security Awareness Training. No obstante, les cuesta mucho mantener este nivel posteriormente. Esto se debe, por una parte, al aumento en el grado de dificultad de las simulaciones de phishing a medida que pasa el tiempo, mientras que, al mismo tiempo, cada vez se van incorporando más empleados a la formación. Por eso es conveniente que las empresas se mantengan en un ciclo de formación continua permanente.

Igualmente ilustrativa es la conclusión de que los escenarios de phishing que más prosperan son aquellos que aprovechan la confianza que tienen los empleados en la autoridad como factor psicológico para ejercer una influencia sobre ellos. En este punto se apela especialmente a los cargos directivos para que den ejemplo en el ámbito de la seguridad informática. Deben animar a los empleados a participar en el Security Awareness Training y compartir sus experiencias.

Capítulo 2: Phishing - el líder de los ciberataques

El phishing se ha convertido en una amenaza omnipresente. El Departamento de Ciberdelincuencia de la Oficina Federal de Investigación Criminal alemana (BKA, por sus siglas en alemán) ha registrado un significativo aumento de las cifras relativas al phishing en 2021 y clasifica el fraude por mensajes de correo electrónico como uno de los tipos más frecuentes de ciberataques.[1]

Según esto, más de un 90 por ciento de todos los ciberataques se inician con un mensaje de correo de phishing. Como reveló el informe Hornetsecurity Cyber Threat Report 2021/2022 , un 40 por ciento de todo el tráfico de correo electrónico representa una amenaza potencial.[2] Las opciones van desde envíos masivos indiscriminados hasta mensajes de spear phishing relacionados con personas concretas, para los cuales se espía a la víctima durante semanas o meses con un objetivo concreto.



ATTACK STATISTIC	%
Andere	42.0
Phishing	24.8
URL	16.2
Ransom	7.1
Executable in archive/disk-image	3.9
Advance-fee scam	2.3
Brand Impersonation	2.1
Maldoc (malicious attachment)	1.5

Fig. 1: The most popular email attack tactics in the 1st half of 2021

Graves consecuencias para las empresas

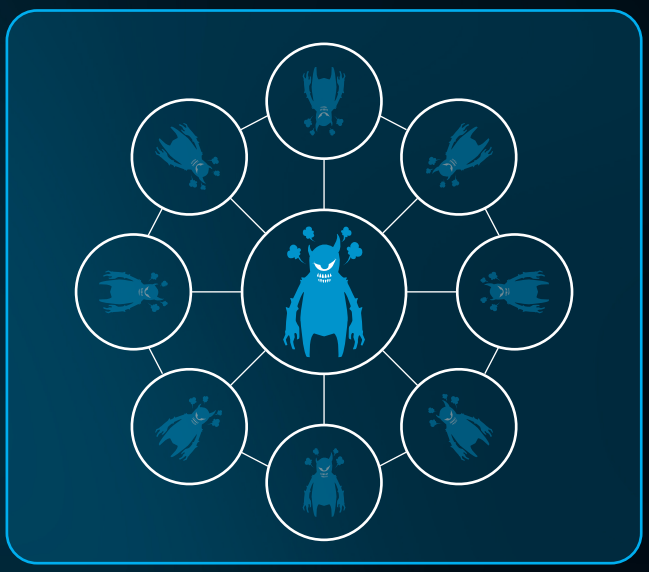
Un ataque de spear phishing realizado con éxito puede suponer graves daños económicos para las empresas afectadas y una pérdida de confianza entre sus clientes y partners. En mensajes de correo electrónico que se hacen pasar por auténticos, los estafadores simulan ser superiores, compañeros de trabajo o partners para persuadir a los empleados de que revelen datos muy sensibles o para que abran enlaces y archivos adjuntos maliciosos. Los empleados pueden ser obligados, en nombre de supuestos directivos, a realizar transferencias de grandes sumas de dinero a cuentas falsas. En otros casos, un ataque exitoso puede servir como puerta de entrada a toda la red de la empresa.

Fig. 2: Damage caused by cybercrime to companies in Germany according to Bitkom.

Sin tregua a la vista

No se prevé una disminución de las cifras actuales de phishing, debido a lo atractivo que resulta este tipo de ataque. Más bien al contrario. La pandemia de coronavirus ha resultado ser un nefasto catalizador, como revela el informe Microsoft Digital Defense Report 2021.[3] Muchos ciberdelincuentes ven la oportunidad de aprovechar los puntos débiles que surgen con la prevalencia cada vez mayor del teletrabajo entre los empleados, así como de las insuficientes medidas de seguridad informática de las empresas.

Otro gran repunte del phishing se dio con el inicio de la invasión rusa de Ucrania. Entre otros, los ciberdelincuentes se hicieron pasar por entidades bancarias, simulando tener que comprobar si los clientes cumplían con las sanciones de la UE contra Rusia, haciéndose con sus datos de registro a través de páginas web falsificadas de los bancos. Para la falsificación de las pantallas de entrada no necesitan tener conocimientos de programación, sino que pueden hacer uso de kits de phishing que se pueden adquirir en la dark web por poco dinero o incluso gratis. Con estas herramientas a su disposición, los estafadores son capaces incluso de esquivar la autenticación de dos factores (2FA) convencional, que hasta ahora era considerada uno de los métodos más eficaces para proteger las cuentas online.



Bandas de estafadores activas en todo el mundo

Los ejemplos muestran que los atacantes de phishing tienen cada vez menos escrúpulos y que sus métodos son cada vez más sofisticados. Así, aumentan los delitos cometidos por bandas de estafadores internacionales, que cuentan con cientos de miembros y aúnan amplios conocimientos técnicos para cubrir de manera profesional toda la cadena del ataque. Según la BKA, cada vez son más los actores que ofrecen incluso ataques selectivos de phishing siguiendo un modelo de «Crime as a Service», o crimen a demanda.

Dentro de las bandas de ciberdelincuentes hay determinados «expertos» que se ocupan de buscar los datos de posibles objetivos, que se pueden encontrar en las redes sociales y otras fuentes de internet, como los portales de valoración de empleadores o las páginas web de empresas. Precisamente, los usuarios entusiastas de las redes sociales son un objetivo fácil para los estafadores mediante spear phishing, como ha demostrado un estudio conjunto de la Technische Universität Darmstadt e IT-Seal.[4] Así, los estafadores usan a menudo los datos de perfil que son de acceso público, como empleo actual, formación, aficiones o contactos para, a partir de ellos, diseñar mensajes de spear phishing personalizados.

Asimismo, los miembros de las bandas encargados de diseñar los mensajes falsificados tienen un rol especial. Aparte de simular tener conocimientos del entorno personal, deben dominar los trucos de manipulación psicológica para engañar a sus víctimas. Ya sea a través de la confianza en la autoridad, la curiosidad, las ganas de ayudar, las prisas o el miedo, sintiéndose seguros de que el destinatario del mensaje seguirá sus indicaciones sin pararse a pensar.

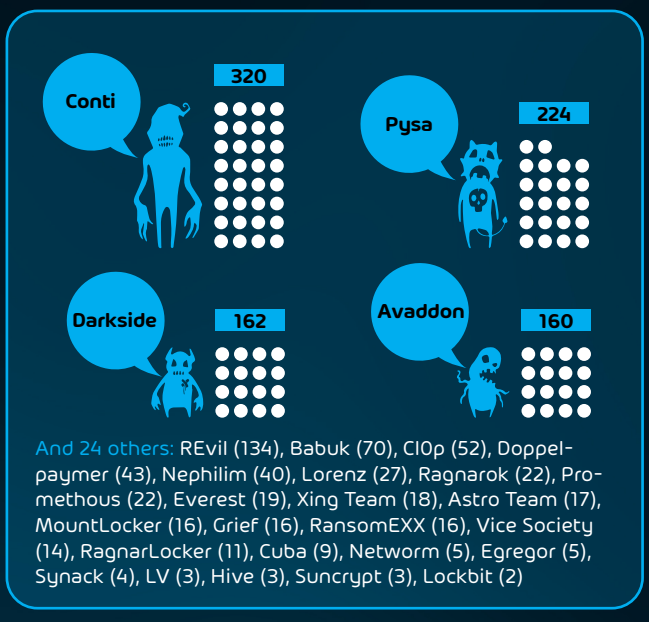


Fig. 3: The fraud gangs with the most published leaks of stolen or extorted personal data

Capítulo 3: El Employee Security Index (ESI®) referencia para el progreso en el aprendizaje

Hornetsecurity ofrece una formación en concienciación sobre seguridad que combina contenidos, herramientas y métodos didácticos para proporcionar una innovadora oferta de servicios. La característica diferenciadora es el Employee Security Index (ESI®) patentado de IT-Seal, que pertenece al grupo Hornetsecurity desde mayo de 2022. Con él se facilita un índice de referencia con base científica, que permite medir y supervisar objetivamente el comportamiento de los empleados en materia de seguridad.

Esto no era posible con los enfoques de medición que había hasta ahora, ya que estos no permiten una estandarización. Por ello no se podía llevar a cabo una comparación en periodos largos de tiempo o entre diferentes departamentos, funciones o localizaciones de la empresa. Esto también llevaba aparejado el riesgo de sobrestimar o infravalorar los problemas individuales de seguridad, los errores o los clics en mensajes de correo electrónico de spear phishing, impidiendo que la empresa obtuviera un conocimiento transparente del comportamiento de sus empleados en lo que respecta a la seguridad. Por eso, muchas veces se realizan inversiones inadecuadas, bien por ser excesivas o bien por ser insuficientes, para alcanzar un nivel adecuado de seguridad.

El tiempo de preparación es decisivo

El ESI®, por el contrario, representa un método realista y replicable para medir la concienciación en seguridad. Para calcular el ESI® se clasifican los ataques de spear phishing en diferentes categorías (llamadas «niveles») según el tiempo que necesitan los ciberdelincuentes para prepararlos y llevarlos a cabo. Este esfuerzo se compone, entre otros elementos, de la adquisición de información de fuentes de acceso público, la preparación técnica, la copia de diseños de páginas web, así como la puesta a punto de la infraestructura informática necesaria para llevar a cabo un ataque de phishing. De este modo, se diferencian siete categorías, que se corresponden con un tiempo de preparación que puede ser desde una hora hasta varios días y semanas. El ESI® individual de una empresa es la consecuencia de la manera en que reaccionan sus empleados a las simulaciones de phishing en diferentes grados de complejidad.

Para poder clasificar de manera estandarizada el nivel de seguridad de una empresa, Hornetsecurity ha definido los valores de tolerancia de un comportamiento ejemplar en materia de seguridad. Estos valores se basan en las «tasas de éxito» desde el punto de vista del atacante. Como una «tasa de éxito» 0 es irreal (todo el mundo comete errores), cada valor de tolerancia se sitúa en el punto medio entre la seguridad y la viabilidad. Un grupo de estudio modélico con la «tasa de éxito» mínima obtiene, en una escala del 0 al 100, como mínimo un ESI® de 90. Si se da un comportamiento sensible con el doble de frecuencia, el grupo obtiene un valor de ESI® de 80; si la frecuencia es del triple, entonces el valor es de 70. Los resultados menores de 70 se consideran peligrosos. Los valores de tolerancia definidos por Hornetsecurity se basan en el estado actual de la investigación y en los valores empíricos obtenidos de simulaciones de phishing en empresas de muy diversos sectores.

De este modo, el ESI® ofrece a las empresas un índice concreto y fiable para comparar de forma estandarizada los diferentes grupos de empleados entre sí. ¿Dónde existe una mayor seguridad, en Ventas o en Recursos Humanos? ¿Y en qué punto se encuentra la gerencia en comparación con el departamento de contabilidad? Esta información es muy valiosa a la hora de determinar las medidas selectivas de formación.

Capítulo 4:

INFORME ESI®
CONCLUSIONES MÁS IMPORTANTES Y PRÁCTICAS RECOMENDADAS

Este informe muestra la eficacia del ESI® para medir y optimizar la concienciación en seguridad de los empleados. Para ello se evaluaron 1,8 millones de ataques simulados de spear phishing realizados entre mayo de 2019 y junio de 2022 a unos 140.000 usuarios de 350 empresas de todos los tamaños y sectores.

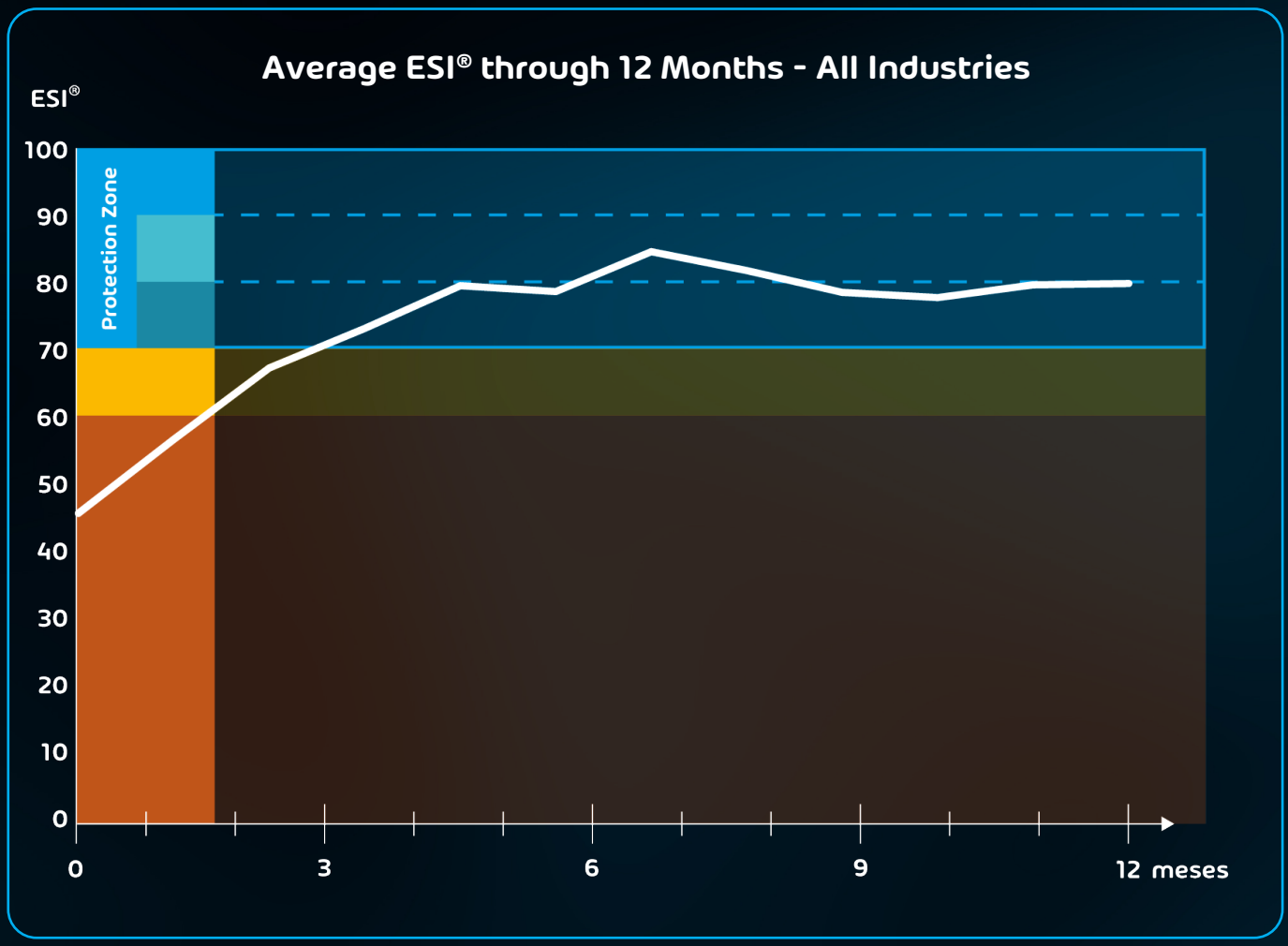
Se tuvo en cuenta el comportamiento de cada uno de los usuarios a lo largo de una capacitación de doce meses. Quedó patente la influencia que tienen en la tasa de clics, entre otros, la pertenencia a un sector, la función y la posición de un empleado dentro de una empresa. Igualmente se analizó el efecto de factores externos, como el paso del tiempo, las pausas realizadas en la formación y la aplicación de trucos psicológicos. Los resultados del índice de referencia ESI® revelan cuál es el nivel óptimo de conciencia en seguridad en los diferentes grupos de usuarios que se puede alcanzar con las distintas medidas formativas de concienciación.

A continuación se presenta una breve selección.

HORNETSECURITY

IT-SEAL
Part of HORNETSECURITY group

Análisis 1: Curva media de ESI®



Es necesaria una formación continua en concienciación

La curva media del ESI® a lo largo de 12 meses muestra claramente lo importante que resulta una formación continuada en concienciación de seguridad para los empleados. Solo si se repiten con regularidad las simulaciones de spear phishing y se van adaptando estas continuamente a los métodos actuales de ataque se puede mantener un alto nivel de seguridad durante un periodo prolongado de tiempo.

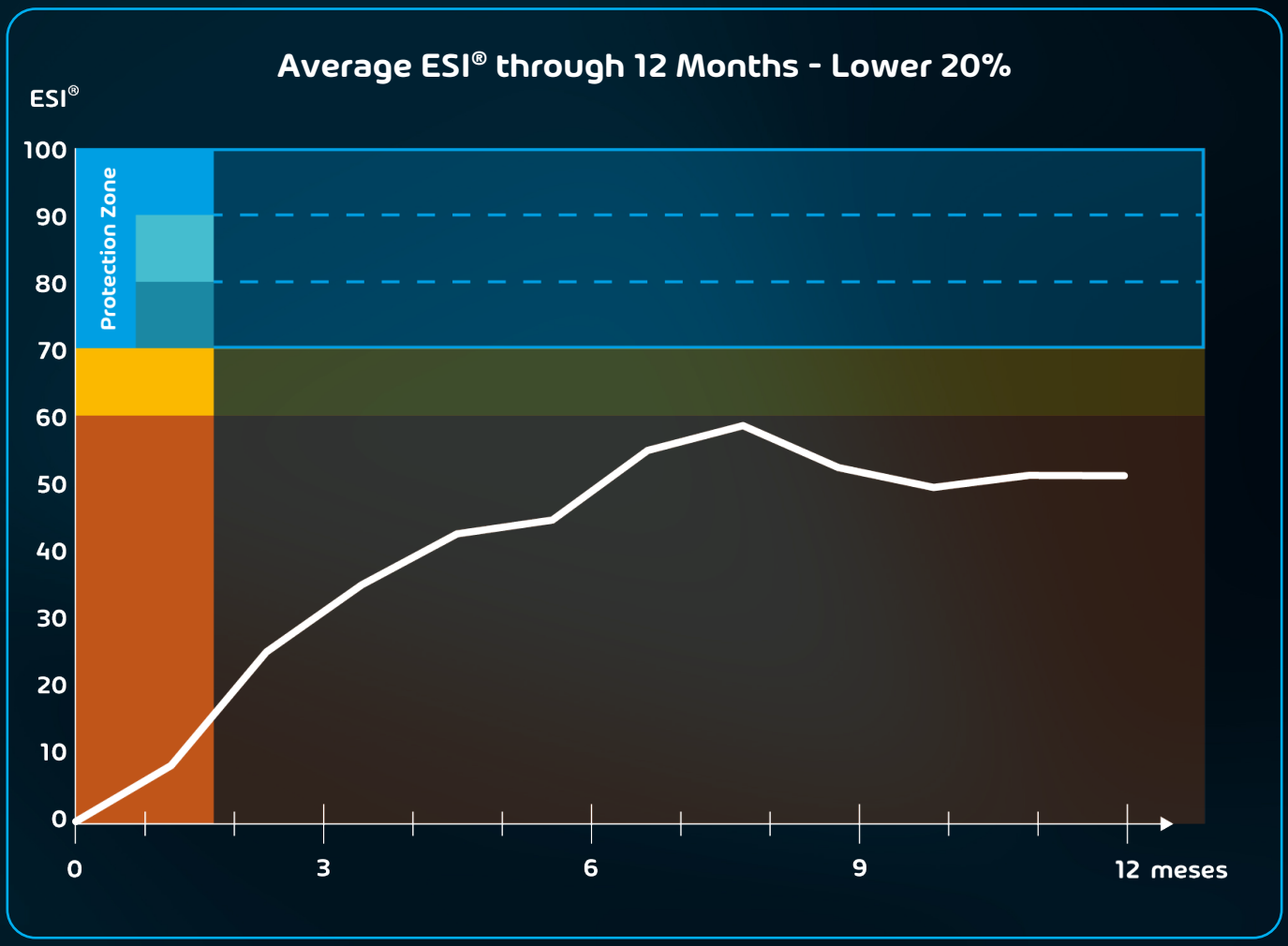
Como se muestra en el gráfico, al principio del entrenamiento, la curva del ESI® asciende rápidamente y, al cabo de una media de tres meses, alcanza un nivel de seguridad aceptable. Pero a las empresas y organizaciones les cuesta mantener este nivel a largo plazo. Esto se debe, por una parte, a que con el paso del tiempo los empleados olvidan las lecciones aprendidas durante las simulaciones de spear phishing.

Por eso, para que los empleados estén actualizados, las empresas y organizaciones deberían apostar por una formación permanente. Solo repitiendo con regularidad la recreación de los ataques de spear phishing se garantiza que los empleados reconozcan la importancia de la información recibida y la recuerden a largo plazo.

Por otro lado, las compañías siempre están incorporando a nuevos empleados, que deben tomar conciencia de los peligros que entraña el phishing y recibir una capacitación en el reconocimiento de mensajes fraudulentos de correo. Mediante las campañas continuas de concienciación se puede incorporar sin problema a los recién llegados en la formación y fortalecer su propia responsabilidad en materia de seguridad informática.

¡Aprende más!

Análisis 2: el ESI® del «20 % inferior»



¡Nada de café para todos!

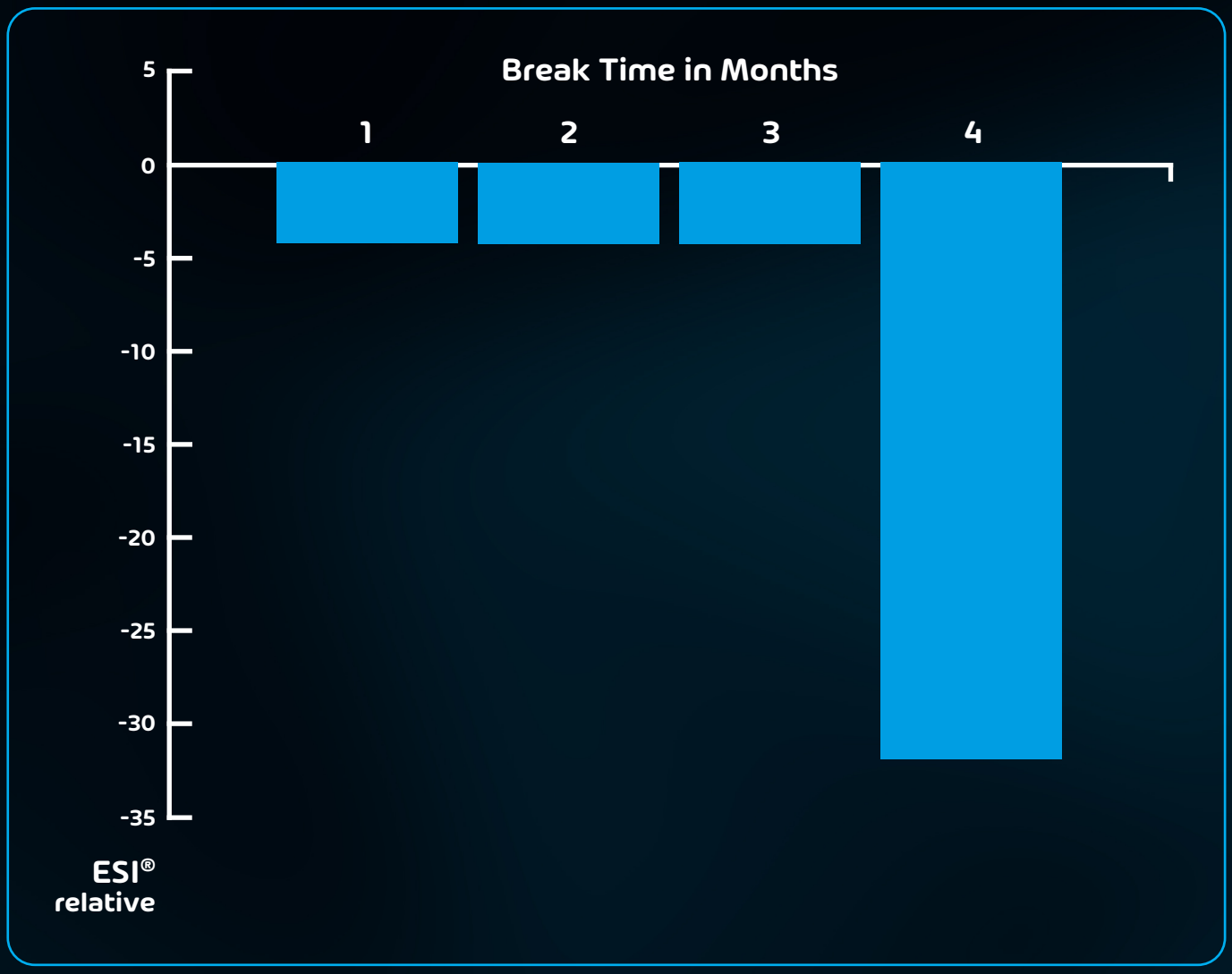
La fuerza de una cadena se determina por la de su eslabón más débil. La trayectoria del ESI® de los llamados del «20 % inferior» muestra precisamente que esta conclusión se aplica también al «cortafuegos humano» para referirse a la protección contra los maliciosos ataques de spear phishing. Estamos hablando de los grupos de usuarios que muestran las mayores tasas de clics en este tipo de simulaciones.

Si bien también en los del «20 % inferior» se manifiesta cierto efecto de aprendizaje en un periodo de 12 meses, como se observa en la curva mostrada anteriormente, durante este periodo el grupo no alcanza ni una sola vez un nivel adecuado de seguridad (es decir, un ESI® de, al menos, 70). Y esto ocurre a pesar de que los del «20 % inferior» recibieron la misma formación en concienciación de seguridad que sus compañeros y compañeras.

Los resultados del análisis muestran claramente que la capacitación en seguridad no se debe impartir del mismo modo para todos, sino que debe orientarse en función de las necesidades individuales de aprendizaje de los empleados, ya que no todos los usuarios aprenden de la misma manera, ni a la misma velocidad ni alcanzan el mismo nivel.

El ESI® permite que las empresas aborden las diferentes necesidades de aprendizaje de sus empleados de forma rápida y sencilla. Ofrece un índice concreto y fiable para documentar los avances personales en la formación y adoptar aquellas medidas de capacitación que resulten adecuadas y precisas. Si los usuarios muestran unas tasas de clics elevadas, como los del «20 % inferior», deben recibir una formación más intensa.

Análisis 3: caída del ESI® tras un paréntesis en la formación



Pausas en la formación para adquirir conocimientos duraderos

La concienciación en seguridad de los empleados se puede comparar con un músculo que se relaja si no se entrena con regularidad. Cuando un grupo o un empleado interrumpe la formación durante un tiempo y la retoma más adelante, se evidencia un claro deterioro en su comportamiento de seguridad. Estos usuarios parecen haber olvidado contenidos didácticos importantes de las simulaciones de spear phishing, y muestran más debilidad en la gestión de estas amenazas.

La caída del ESI® en este gráfico muestra el alcance de este efecto (no se han tenido en cuenta los del «25 % inferior y superior», es decir, grupos de usuarios con tasas de clics especialmente bajas o elevadas). Ya tras el primer mes de pausa en la formación, el ESI cae cinco puntos, situándose a menudo por debajo del nivel de seguridad que se pretende lograr. A los cuatro meses sin capacitación, el ESI® ya ha sufrido un descenso de más de 30 puntos. En la práctica, esto significa que las empresas vuelven casi a la casilla de salida en lo que respecta al comportamiento de seguridad de sus empleados.

Pero las pausas breves en la formación también pueden suponer una ventaja pedagógica y didáctica para las empresas. Si determinados grupos o trabajadores han alcanzado una vez el nivel de seguridad deseado, deberían interrumpir la formación a propósito durante un periodo de entre dos y tres meses. Se ha demostrado que el aprendizaje adquirido tiene un efecto más duradero en el comportamiento de seguridad si se actualiza tras haber hecho una pausa. Además, así se evita un posible desgaste en la conducta de seguridad de los empleados.

Análisis 4: el sector tecnológico frente a la media

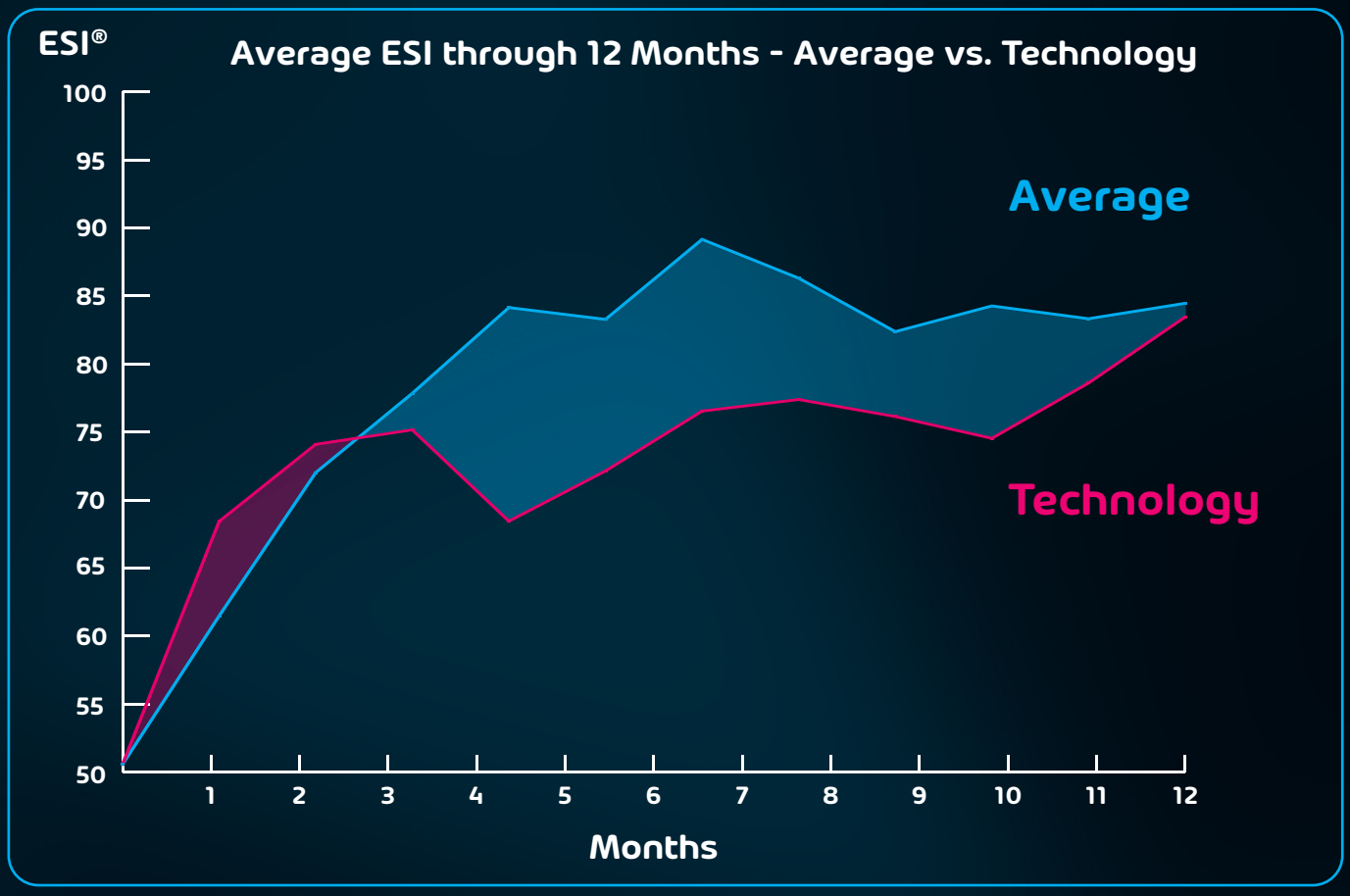


Abb. X: Technologie-Sektor vs. Durchschnitt ESI® Verlauf über 12 Monate

¿Afín a la tecnología? Clara sobrestimación de la propia actitud

En realidad, sería razonable pensar que los empleados de las empresas tecnológicas están mucho más preparados que los de otros sectores a la hora de afrontar riesgos cibernéticos. Pero esta suposición es engañosa, como se puede ver más arriba en las curvas de la trayectoria del ESI®. Según estas curvas, el sector de la tecnología muestra unas tasas de clics mucho más elevadas que el promedio general.

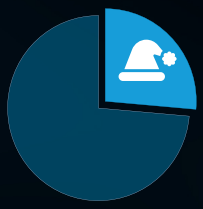
Esto se debe a que las personas suelen sobrestimar sus propias capacidades, especialmente cuando se trata de temas con los que están familiarizadas profesionalmente. En el sector tecnológico, esta actitud puede suponer riesgos considerables para la seguridad, no solo dentro de la propia empresa, sino también para sus clientes. En este sector trabajan muchos proveedores de software y centros de datos que desarrollan y mantienen aplicaciones para otras empresas.

También en este caso, el ESI® ayuda a compensar las carencias específicas del sector en el comportamiento de seguridad. Las empresas tecnológicas cuentan así con un índice fiable para averiguar cuál es el nivel de seguridad y cómo está siendo el progreso formativo de sus empleados, así como para adoptar otras medidas de capacitación precisas. De este modo, el Awareness Training puede adaptarse sistemáticamente a las necesidades de aprendizaje de los empleados en el sector tecnológico, que son más elevadas.

Análisis 5: el «top 5» de los escenarios de spear phishing y sus factores psicológicos

1. Autoridad del remitente y curiosidad

La gerencia informa por correo electrónico sobre un nuevo organigrama con los nuevos cargos de responsabilidad en la empresa. Se puede descargar en la Intranet.
tasa de éxito del 28%

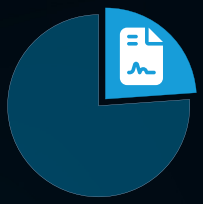


2. Autoridad del remitente y curiosidad

Navidad: la dirección regala sus libros favoritos del año a todos los empleados.
tasa de éxito del 28%

3. Miedo a consecuencias desagradables

Se comunica al destinatario que su buzón de correo electrónico está lleno. Puede obtener ayuda siguiendo un enlace.
tasa de éxito del 24%



4. Sentido del deber y miedo a consecuencias desagradables

Se solicita al destinatario que firme las nuevas directivas de teletrabajo.
tasa de éxito del 24%

5. Curiosidad y miedo

El destinatario se entera de que algunos coches que están en el aparcamiento de la empresa han sufrido daños. En las fotos adjuntas podrá comprobar si su vehículo es uno de ellos.
tasa de éxito del 24%

A todos nos motiva algo concreto

Que una persona caiga en según qué tipo de mensaje de spear phishing depende de una gran variedad de factores: el nivel de estrés y formación del usuario, la capacidad de concentración, la apariencia del mensaje, el campo del asunto, etc.

Pero los factores de influencia psicológica tienen una relevancia destacable y cada persona reacciona a ellos de manera diferente. Por ejemplo, hay usuarios que tienden a seguir a la autoridad y abren enseguida todos los mensajes de correo que recibe, supuestamente, de su superior o de la gerencia. Por otro lado, otros empleados se activan más con factores que apelan a la buena disposición o al sentido del deber.

La curiosidad, el miedo, la confianza en la autoridad, la disposición a ayudar, la vanidad y muchos otros sentimientos son importantes factores psicológicos de influencia para los estafadores. Estos los usan a propósito y muchas veces combinados también de forma individual para embaucar a sus potenciales víctimas. Para que los empleados hagan exactamente lo que se les pide, los ataques de spear phishing se dirigen hábilmente al sistema de pensamiento rápido, como expone el psicólogo y premio Nobel Daniel Kahneman en su bestseller sobre el pensamiento lento y racional.[5]

Por eso, las simulaciones eficaces de phishing siempre deben estar orientadas a los factores de influencia ante los cuales un usuario resulta más vulnerable. De esta manera, los empleados aprenden durante la formación a prepararse conscientemente contra los trucos psicológicos de los atacantes a los que son especialmente receptivos.

Capítulo 5: Atención, empresas: es necesario actuar rápido

Como muestran los modelos, los crecientes riesgos del phishing requieren una actuación rápida por parte de las empresas. Estas deben afrontar el hecho de que incluso la tecnología más avanzada en seguridad informática por sí sola no basta para protegerse del spear phishing, ya que, aunque hoy en día los departamentos de sistemas consiguen bloquear millones de mensajes de correo engañosos, algunos de estos logran llegar a las bandejas de entrada de los empleados.

Por eso, las empresas deberían contemplar el refuerzo del rol de los empleados como cortafuegos humano como una tarea urgente. Este requisito también está respaldado por un estudio actual de la asociación digital bitkom, según el cual gran parte de los ciberdelincuentes aprovechan el factor humano como el eslabón supuestamente más débil de la cadena de seguridad.[6]

Lo más eficaz es una estrategia de seguridad informática que integre los tres pilares centrales de una cultura de seguridad: mindset, skillset, toolset (actitudes, habilidades, herramientas). Esto significa, concretamente, que los empleados deben concienciarse ante la amenaza que suponen los mensajes de spear phishing, formarse para reconocerlos y recibir apoyo para defenderse con las medidas técnicas y organizativas adecuadas.

Mindset

Motivation and open communication

- Understanding the threat
- Emphasize personal responsibility
- Communication tools for all stake holders

Skillset

Acquiring skills and knowledge

- Phishing Simulation
- E-Learning
- Online seminars
- Face-to-face training
- Awareness materials

Toolset

Actively getting involved and intervening

- Live-Dashboard
- Password manager
- Safety message chains
- Reporter-Button Outlook Add-In

Mindset: desarrollar el olfato ante el peligro

La confianza ciega en la tecnología de seguridad informática está muy extendida entre los trabajadores. Los mensajes de correo se abren sin pensar y se siguen las indicaciones, especialmente cuando parecen proceder de fuentes fiables. Por eso las empresas harían bien en impulsar un replanteamiento en el que apelen a la propia responsabilidad y autoeficacia de los empleados. Estos deben interiorizar que su intervención y su atención son una contribución determinante al funcionamiento de toda la empresa.

Para prepararse en la concienciación sobre seguridad, se recomienda que la administración inicie campañas informativas que cuenten con el respaldo de los cargos directivos y de los responsables de seguridad informática. La experiencia muestra que las cifras y los datos sobre los incidentes de seguridad en el propio sector provocan un efecto duradero en los empleados. Por ejemplo, FACC, el fabricante austriaco-chino de maquinaria, perdió unos 43 millones de euros cuando un contable fue engañado con mensajes de correo falsos provenientes del supuesto CEO de la empresa. Transfirió esta suma a estafadores en internet que le hicieron creer que se trataba de transacciones estrictamente confidenciales para la adquisición de una compañía.

Las campañas informativas logran su máximo impacto si se despliegan en diferentes canales y si incluyen reuniones de equipo, vídeos y circulares.

Skillset: fomento de las decisiones intuitivas

Las subsiguientes capacitaciones en seguridad informática no deberían limitarse a los clásicos como la formación presencial, la formación online y los webinars, ya que estas formas de aprendizaje solamente transmiten conocimientos teóricos sobre los ataques de phishing. Para estimular la intuición de los usuarios en la rutina diaria, las simulaciones prácticas de spear phishing han demostrado su validez, utilizando datos reales de los empleados y de la empresa para imitar ataques reales. Si un trabajador es engañado por un mensaje de correo electrónico falso, se le redirigirá a una página explicativa interactiva que ofrece advertencias sobre las características sospechosas del mensaje: desde un par de letras cambiadas en el campo del destinatario, hasta los enlaces y adjuntos sospechosos, pasando por los subdominios falsificados.

Las simulaciones de spear phishing son tan eficaces porque estimulan las decisiones impulsivas de los empleados, que son los que hacen clic espontáneamente en estos mensajes de correo. En su bestseller Pensar rápido, pensar despacio, el psicólogo y premio Nobel Daniel Kahneman diferencia este sistema de pensamiento instintivo y emocional del ser humano de su capacidad racional y lógica de tomar decisiones.[6] Además, la recreación de los ataques de spear phishing se aprovechan del «Most Teachable Moment» del empleado: al recibir, justo en el momento adecuado, una explicación sobre lo perjudicial de su conducta, está obteniendo una formación especialmente eficaz para reconocer el ataque y en el futuro actuará con mayor prudencia ante un nuevo mensaje de correo.

Para que se mantenga este efecto del aprendizaje, se deberían repetir continuamente los ataques simulados de spear phishing que, a su vez, deben estar siempre adaptados a los nuevos métodos de ataque. De otro modo, lo aprendido cae rápidamente en el olvido, como descubrió el psicólogo Hermann Ebbinghaus ya en 1885.[8] Según la curva de olvido de Ebbinghaus, el contenido formativo se debe repetir varias veces para que quede grabado de modo permanente. Con la frecuencia de la repetición, el cerebro reconoce la importancia de la información y la almacena en la memoria a largo plazo. Según esto, la formación en Security Awareness debe convertirse en un proceso continuo si pretende tener un efecto duradero.

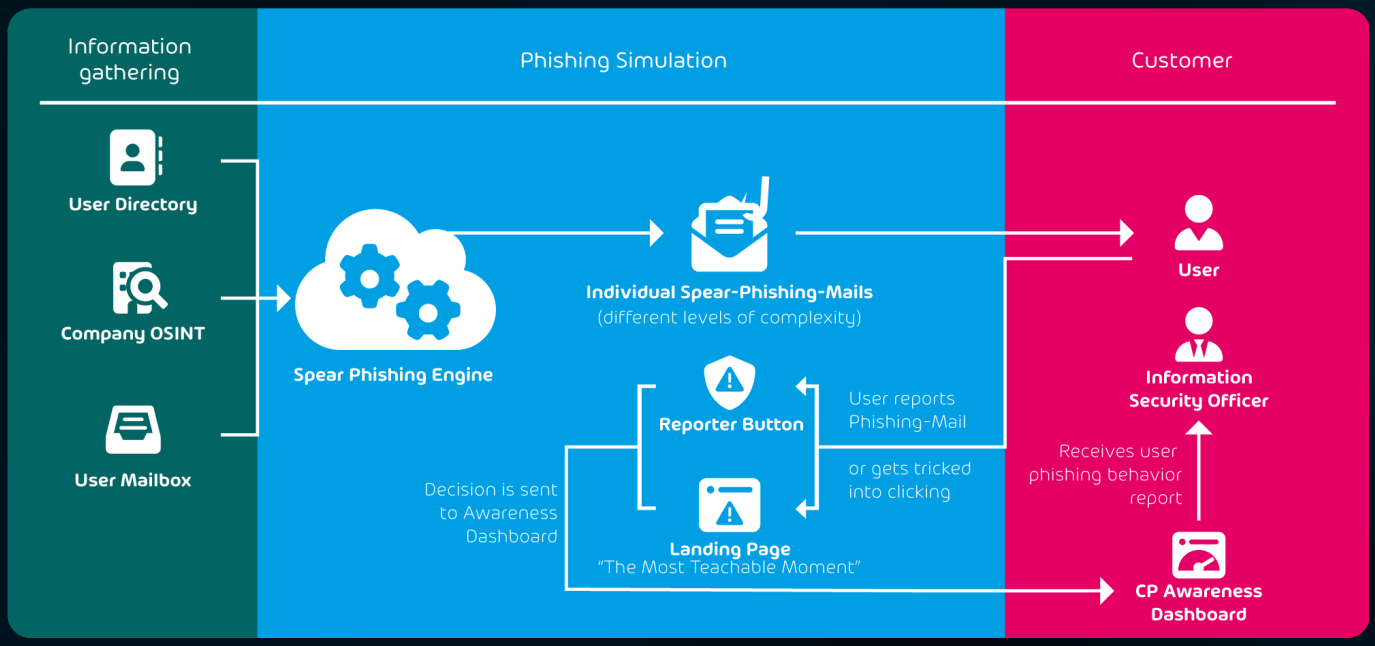


Fig. 4: Spear phishing simulation process

¡Aprende más!

Toolset: la guinda de toda estrategia de defensa contra el phishing

Las empresas pueden completar su defensa contra el spear phishing si cuentan con las herramientas adecuadas. Los gestores de contraseñas ofrecen una gran ventaja, ya que se integran fácilmente en el entorno informático de trabajo y permiten almacenar y administrar las identidades digitales de forma centralizada. Estas herramientas contribuyen a evitar que los trabajadores utilicen siempre los mismos datos de inicio de sesión por comodidad. Así, si los atacantes de spear phishing consiguen robar una sola contraseña, no podrán acceder automáticamente a todas las demás cuentas de un usuario.

Para impedir la anulación cada vez más frecuente de la 2FA, las empresas deberían pasarse a FIDO2 (Fast Identity Online).[9] FIDO2 ofrece un proceso innovador de 2FA en el cual el registro para usar un servicio en línea se realiza con un cifrado y no se puede descifrar ni siquiera con los procedimientos actuales de ataques de alta tecnología.

Otra herramienta útil es el «Reporter Button», que se puede integrar directamente en Microsoft Office y que ayuda a los empleados a identificar y notificar mensajes de correo dudosos. Con un clic, los usuarios reciben indicaciones útiles sobre si un mensaje puede haber sido falsificado y, en caso de ser necesario, lo reenvían a los responsables de seguridad informática para que lo comprueben.

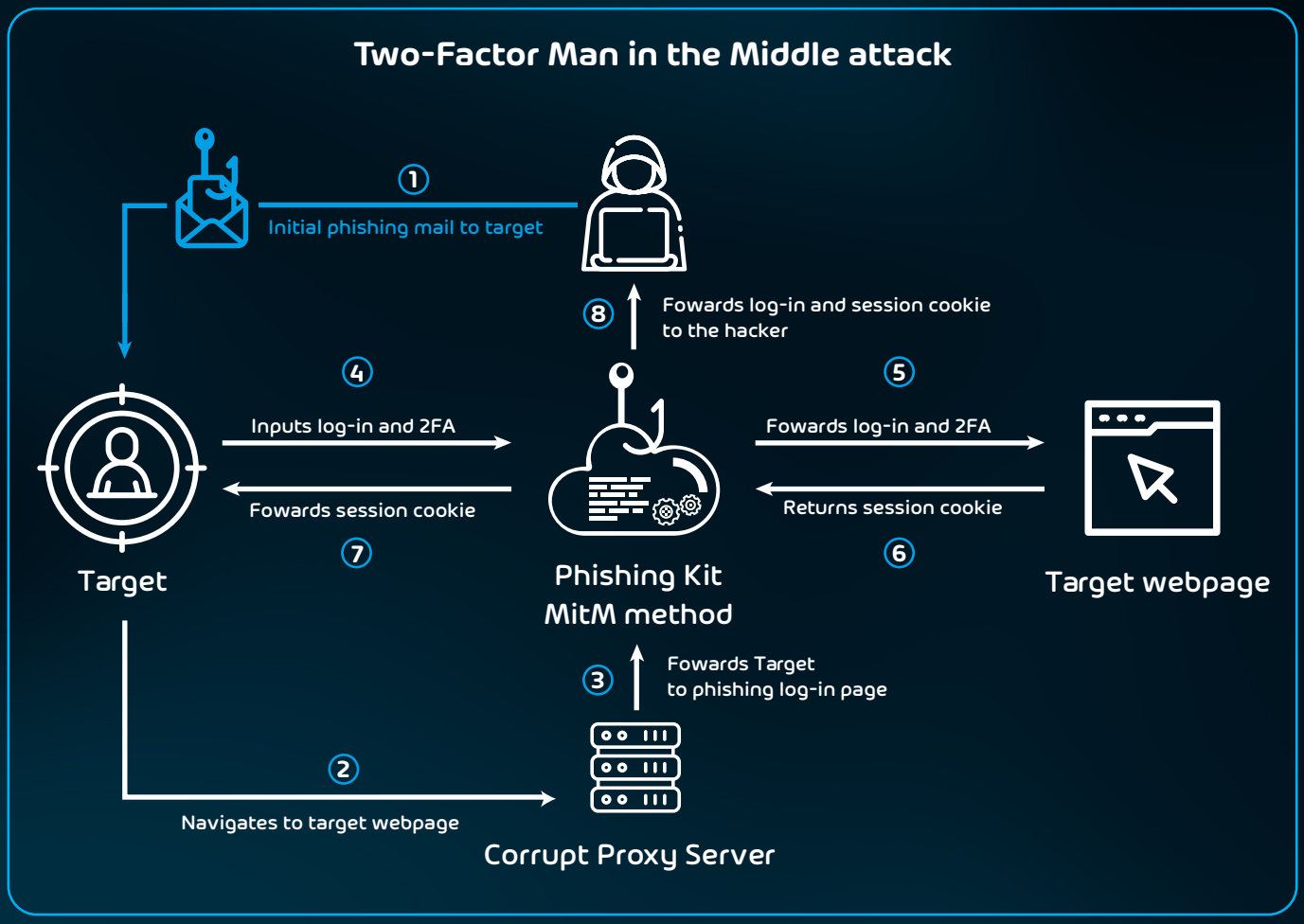


Fig. 5: Building a Man in the Middle Attack against 2FA Authentications

El Security Awareness Service de Hornetsecurity ofrece una solución completa

Para llevar a cabo la formación en Security Awareness, Hornetsecurity ha desarrollado una solución completa que combina formatos innovadores de aprendizaje (formación en línea, «Most Teachable Moment», gamificación) con una de las simulaciones de spear phishing más avanzadas. En el marco de la formación clásica online, los vídeos breves y los cuestionarios, los participantes reciben información importante sobre los crecientes riesgos cibernéticos y sobre la mejor manera de protegerse.

En los ataques simulados de phishing interviene el Spear Phishing Engine patentado, que hace que los ataques resulten engañosamente auténticos. El Spear Phishing Engine está basado en innovadoras tecnologías de inteligencia de fuente abierta (OSINT, por sus siglas en inglés), que generan de forma automatizada escenarios de phishing específicos para empresas, departamentos y empleados. Para dar contenido a los ataques de phishing se utilizan datos de la empresa que son de acceso público (por ejemplo, de portales de empleo de la compañía) y otras fuentes.

Esto permite elaborar mensajes de correo realistas en los que, por ejemplo, el jefe de departamento realiza una consulta sobre una factura que se adjunta. En otros mensajes, los estafadores se camuflan como compañeros de trabajo y hacen referencia a una supuesta conversación que se tuvo sobre un tema específico. El destinatario del mensaje recibe un enlace «interesante» para que profundice en el tema, pero que en realidad lleva directamente a un software malicioso. Los ejemplos muestran que los atacantes de spear phishing siempre recurren al mismo truco: rebuscan en el baúl de los trucos psicológicos y apuntan a los sentimientos de sus posibles víctimas con tanta habilidad que estos, sin pensarlo, hacen exactamente lo que los ciberdelincuentes les piden.

SECURITY AWARENESS SERVICE

¡Aprende más!

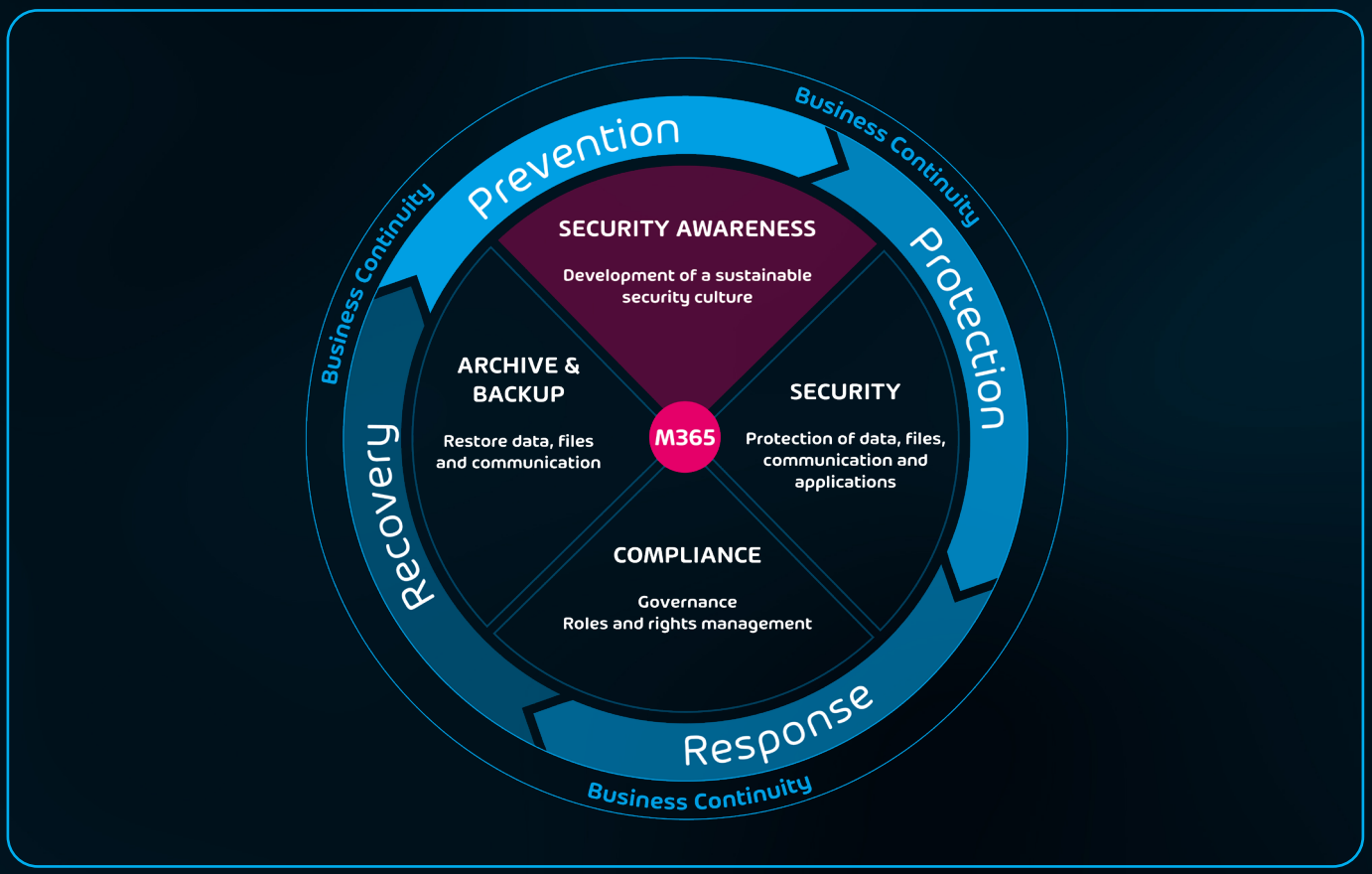


Abb. 6: Security Awareness als Teil der Business Continuity von Hornetsecurity

La formación en piloto automático

Al inicio del Security Awareness Service se debería aspirar a un nivel de seguridad mínimo de un ESI® 70, para que luego vaya aumentando progresivamente. Para alcanzar el ESI® correspondiente se pone en marcha el Awareness Engine. Este motor basado en IA permite la formación en piloto automático, pausando e iniciando automáticamente los ataques de spear phishing sobre la base de las referencias del ESI® y las necesidades específicas.

En lugar de asistir a una formación indiferenciada que siga una metodología de formación uniforme, cada usuario recibe tanta formación como necesita y en la menor cantidad posible. Las empresas ahorran tiempo, dinero y valiosos recursos humanos, ya que no deben hacerse cargo de la gestión y mantenimiento de la formación.

A determinados intervalos, se van repitiendo y actualizando los ataques de phishing a los diferentes empleados. Desde el Awareness Dashboard, que, como todas las demás soluciones de Hornetsecurity está integrado en el Control Panel, los gerentes y responsables de seguridad informática pueden ir informándose de cómo se va desarrollando la capacitación y de la evolución del índice ESI®. De igual modo, los propios empleados pueden seguir su progreso individual de aprendizaje en el llamado User Panel. Se trata de la plataforma de aprendizaje de Security Awareness Service, para la que cada participante cuenta con un acceso propio que le permite ver sus resultados individuales.

Una formación continua para un éxito duradero

Ya son más de 1.000 las empresas de todos los sectores y tamaños que confían en la tecnología probada de IT-Seal, perteneciente al grupo Hornetsecurity.

Para alcanzar un efecto duradero a largo plazo, muchos clientes se deciden por una implementación permanente del Awareness Training. Así se puede evitar, por un lado, que el nivel de ESI® alcanzado caiga en picado.

En lugar de ello, se puede fijar la concienciación sobre seguridad en la memoria a largo plazo de los participantes. Por otro lado, de esta manera es posible ir integrando a los nuevos empleados en la formación en seguridad.

Capítulo 6: Casos de éxito: cómo los clientes se benefician de Security Awareness Service

Los ataques de spear phishing que prosperan pueden acarrear consecuencias fatales para las empresas, ya sean estas del sector de las finanzas, los seguros o la industria. A continuación, vemos cómo dos prestigiosas empresas refuerzan sus defensas con ayuda de Security Awareness Service.

Como proveedor líder en Alemania de soluciones online multibanco y para banca móvil, Star Finanz opera en el sector financiero, un entorno sujeto a una fuerte regulación. Es frecuente que la empresa maneje datos sensibles relacionados con las finanzas y las transacciones de sus clientes particulares y empresas. Para protegerlos del spear phishing, en el pasado ya se habían llevado a cabo capacitaciones internas para los empleados.

Pero el nivel de perfeccionamiento de los ataques de phishing motivó que se buscase la ayuda de un proveedor profesional de formación. La elección de Security Awareness Service de Hornetsecurity se debió a que es una solución completa que está en consonancia con las últimas actualizaciones de los atacantes. A esto se le añade el innovador índice ESI®, que permite medir objetivamente la concienciación en seguridad de los empleados.

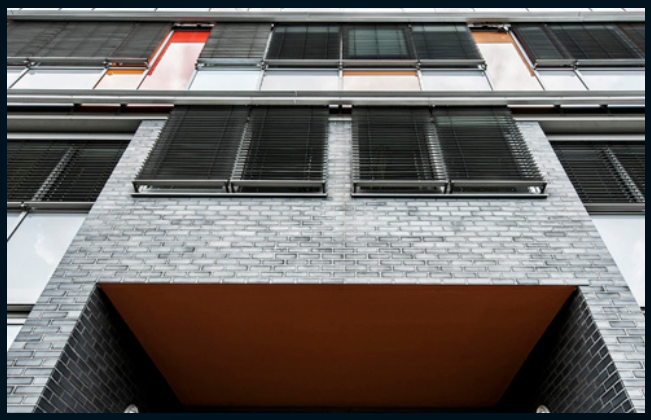
starfinanz

Un progreso formativo apreciable y medible

Aún hoy se siguen realizando continuamente ataques simulados de spear phishing y formaciones online para los empleados de Star Finanz. «Se han logrado grandes avances en el aprendizaje, y el nivel de seguridad del personal ha aumentado significativamente», resume André Haase, Senior Security Architect en Star Finanz.

Por motivos legales de protección de datos, a Star Finanz le resulta muy beneficioso que Hornetsecurity procese los datos de los clientes en el mismo país. Así, las medidas formativas son compatibles con el RGPD de la UE. Además, al emplear las reconocidas medidas de seguridad de Security Awareness Training, la empresa puede establecer una sólida base de cara a una posible certificación en ISO 27001.

Para André Haase está fuera de toda duda que Security Awareness Service seguirá utilizándose a largo plazo para lograr un efecto duradero de la capacitación en seguridad.



André Haase
Senior Security Architect - Star Finanz

Casos de éxito: cómo los clientes se benefician de Training

KIRCHHOFF & LEHR
METALL IN BESTFORM

Cuando una empresa industrial se ve afectada por ataques de phishing, toda la producción puede verse paralizada. La consecuencia es una pérdida de productividad, además de graves daños económicos y reputacionales.

Kirchhoff & Lehr, un especialista conocido en toda Europa por su tecnología de perfilados, no puede permitirse un daño de estas características. Aparte de ofrecer una amplia gama de productos, este fabricante ha conseguido una gran reputación gracias a sus elevados estándares de calidad, su fiabilidad en las entregas y su buena relación calidad-precio. Cuando el número de mensajes maliciosos de correo electrónico aumentó vertiginosamente durante la crisis del coronavirus, la empresa buscó una solución para sensibilizar a sus empleados ante los ataques de phishing.

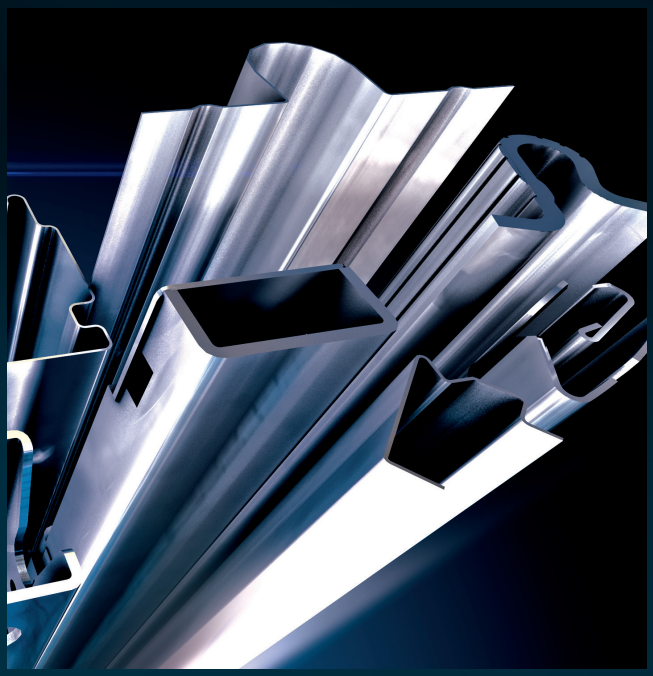
Formación como un activo permanente

Al cabo de poco tiempo, los responsables decidieron establecer el Security Awareness Training como un elemento permanente para los trabajadores de administración. «Sobre todo, lo hicimos por las simulaciones de spear phishing, que proporcionan un gran beneficio pedagógico y didáctico», enfatiza Robert Batz, responsable de IT en Kirchhoff & Lehr.

Antes de que comenzase el Awareness Training, los empleados fueron informados de conformidad con la normativa de protección de datos y se les solicitó su consentimiento. Desde entonces, reciben regularmente mensajes de correo de spear phishing simulados. Se capacita además su conciencia en seguridad a través del Reporter Button, incluido en Security Awareness Service. Si el usuario recibe un mensaje de correo dudoso, puede reenviarlo directamente al departamento de IT para su comprobación.

A los pocos meses, la progresión del ESI® mostró claramente los grandes avances que los empleados habían conseguido a la hora de reconocer los ataques de phishing. Para que mantengan la práctica y también puedan beneficiarse los recién llegados, la formación se ha ampliado más allá de la duración del contrato inicialmente acordada.

Robert Batz, responsable de IT, lo tiene claro: «Los comentarios y opiniones sobre Security Awareness Training han sido abrumadores. Nuestros empleados reconocen la responsabilidad que tienen como cortafuegos humano».



Robert Batz
Head of IT - Kirchhoff & Lehr GmbH

Capítulo 7: Resumen y perspectivas

Incluso con el uso de la tecnología más avanzada, el cien por cien de seguridad no existe. No obstante, las empresas cuentan hoy en día con medidas eficaces para limitar los efectos de los ciberataques. Se puede conseguir que la actividad comercial siga adelante sin interrupciones, que los ataques se encuentren con una rápida defensa y, en caso necesario, que todos los sistemas, archivos y datos puedan ser recuperados con prontitud. Además, la continuidad del negocio permite que las empresas hagan una apuesta segura en lo que respecta al cumplimiento normativo. De esta manera, pueden adoptar las medidas adecuadas para protegerse de procesamientos judiciales o perjuicios a su reputación en caso de sufrir un ciberataque.

Security Awareness se dirige a las personas

Hornetsecurity ya ofrece las soluciones más avanzadas en materia de seguridad de correo electrónico, backup y cumplimiento normativo, cubriendo todos los aspectos del ciclo de seguridad informática: desde la prevención hasta la respuesta y recuperación, pasando por la protección.

Aun así, la mayor parte de los ciberataques siguen centrándose en el «punto débil humano»: al fin y al cabo, hasta los sistemas y herramientas más seguros desde el punto de vista técnico son solo tan seguros como la prudencia con que los manejan los usuarios.

Con Security Awareness Service, Hornetsecurity integra el factor humano en su propia solución de seguridad, incorporándolo activamente en el ciclo de seguridad informática. La capacitación en seguridad continua de Hornetsecurity prepara sistemáticamente a los empleados ante los riesgos cibernéticos, que son cada vez más frecuentes. Con el transcurso del tiempo aprenden a reconocer y repeler de manera efectiva incluso los ataques de phishing más sofisticados; dominan las medidas necesarias para impedir graves incidentes de seguridad y para que en todo momento esté asegurada la continuidad del negocio.

Además, Hornetsecurity ayuda a las empresas a desarrollar el conjunto de actitudes necesarias en materia de seguridad entre los empleados: solo así las habilidades adquiridas en combinación con los procesos y herramientas que las acompañan pueden contribuir a desarrollar una cultura de seguridad activa y duradera.

¡Aprende más!

References

1 Oficina Federal de Investigación Criminal (BKA): Departamento de Ciberdelincuencia 2021, mayo de 2022

2 Hornetsecurity: Cyber Threat Report Edition 2021/2022, enero de 2022

3 Microsoft: Microsoft Digital Defense Report 2021, octubre de 2021

4 Anjuli Franz y Evgheni Croitor, Technische Universität (TU) Darmstadt: Who bites the Hook? Investigating Employees' Susceptibility to Phishing: A randomized Field Experiment, 2021

5 Daniel Kahneman: Pensar rápido, pensar despacio, 2012

6 bitkom: Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr, 5 de agosto de 2021

7 Daniel Kahneman: Pensar rápido, pensar despacio, 2012

8 Wikipedia: Hermann Ebbinghaus

9 Alianza FIDO: Verificación FIDO. Una visión sin contraseñas

Acerca de Hornetsecurity Group

Hornetsecurity es un proveedor líder de seguridad de correo electrónico en la nube y de copias de seguridad, que protege a empresas y organizaciones de de todos los tamaños en todo el mundo. Su galardonada cartera de productos cubre todas las áreas principales de la seguridad del correo electrónico, incluyendo el spamincluyendo el filtrado de spam y virus, la protección contra el phishing y el ransomware, y el archivado y cifrado que cumplen con la ley. archivo y encriptación. Además, hay copias de seguridad, replicación y recuperación de correos electrónicos, puntos finales y máquinas virtuales. El producto estrella es la solución de seguridad en la nube más completa del mercado para Microsoft 365. Con más de 450 empleados en 12 sedes, la empresa, que tiene su sede en Hannover (Alemania), cuenta con una red internacional de socios. Con sede en Hannover, Alemania, cuenta con una red internacional de más de 5.000 socios de canal y MSP, así como con 11 centros de datos redundantes y seguros. Más de 50.000 clientes utilizan los servicios premium, entre ellos Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, DEKRA y CLAAS.

HORNETSECURITY