proofpoint.

LIBRO ELECTRÓNICO

2022

Guía definitiva de la estrategia de ciberseguridad del correo electrónico

Un enfoque centrado en las personas para neutralizar los ataques de ransomware, malware, phishing y fraude por correo electrónico

proofpoint.com/es

Correo electrónico: el vector de amenazas más crítico

Todos los días se libra a nivel mundial una batalla silenciosa en uno de los elementos más populares y esenciales que se utilizan en el trabajo actual: la bandeja de entrada del correo electrónico.

Al ser el principal vector de distribución de malware y terreno abonado para todo tipo de fraudes, el correo electrónico es el canal que cuenta con mayor probabilidad de sufrir ciberataques. Los atacantes engañan a los usuarios para que hagan clic en un enlace no seguro, les proporcionen sus credenciales o incluso lleven a cabo directamente ellos mismos los ataques (por ejemplo, realizando transferencias bancarias o enviando archivos confidenciales).

No es de extrañar que los atacantes muestren preferencia por el correo electrónico. Este medio emplea una arquitectura con décadas de antigüedad que no fue diseñada pensando en la seguridad. Es universal. Y, a diferencia de lo que ocurre con las infraestructuras informáticas y el hardware, los ataques al correo electrónico aprovechan vulnerabilidades que no se pueden corregir con la aplicación de un parche: las personas.

La migración a la nube y el teletrabajo han complicado aún más las cosas.

Las organizaciones gastan miles de millones al año en herramientas de seguridad diseñadas para reforzar el perímetro de la red, detectar las intrusiones y proteger los endpoints. Sin embargo, jamás han llegado a cotas tan elevadas el volumen y el coste del ransomware, las estafas Business email compromise (BEC), el phishing de credenciales y las fugas de datos provocadas por malware[1].

La razón es que los ataques actuales no solo hacen uso de la tecnología, sino que también aprovechan la naturaleza humana. Y el correo electrónico es el camino más fácil para llegar a las personas.

Resultados de recientes investigaciones:

14,8 M$
es el coste anual medio del phishing para una gran empresa, más del triple que la media de 2015[2]

86 %
de las organizaciones sufrió ataques de phishing masivos en 2021[3]

77 %
de las organizaciones sufrió ataques BEC en 2021[4]

78 %
de las organizaciones sufrió ataques de ransomware por correo electrónico en 2021[5]

85 %
de las fugas de datos implican la intervención humana[6]

1 Ponemon Institute. "2021 Cost of Phishing Study" (Estudio sobre el coste del phishing en 2021), junio de 2021.
2 Ponemon Institute. "2021 Cost of Phishing Study" (Estudio sobre el coste del phishing en 2021), junio de 2021.
3 Proofpoint. "State of the Phish 2022", febrero de 2022.
4 Ibid.
5 Ibid.
6 Verizon. "Data Breach Investigations Report" (Informe de investigaciones de fugas de datos - Resumen ejecutivo), mayo de 2021.

Ahora ha llegado el momento de replantearse complemente la situación. El panorama actual de las amenazas exige un enfoque radicalmente nuevo y una estrategia centrada en proteger a las personas, en lugar de la infraestructura.

Esta guía puede servirle de punto de partida tanto si dirige un centro de operaciones de seguridad multinacional como un equipo de seguridad pequeño y compacto. En ella examinamos:

- Por qué el correo electrónico debe ser su principal prioridad en materia de seguridad
- Por qué es tan difícil protegerlo
- Por qué resulta más eficaz una seguridad multicapa integrada y centrada en las personas
- Cómo optimizar las operaciones de seguridad del correo electrónico para ahorrar dinero y simplificar la medidas de respuesta

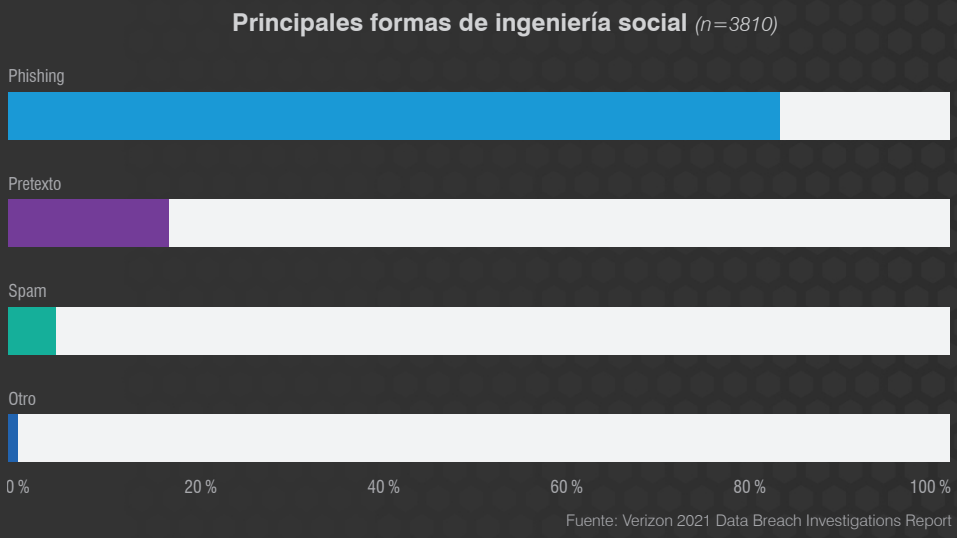


Figura 1: Principales formas de ingeniería social

SECCIÓN 1

Los ciberataques evolucionan con más rapidez que las defensas tradicionales

Proteger el correo es la clave para garantizar la seguridad de la empresa. Sin embargo, el reto es considerable,

ya que las amenazas para el correo electrónico son numerosas y variadas. Las técnicas de ataque evolucionan constantemente. Y la naturaleza humana, el eslabón más débil en toda organización, es el objetivo perpetuo.

No es de extrañar que las soluciones desarrolladas hace dos o tres años para luchar contra los ataques no sean ya eficaces.

Esta sección describe algunos de los métodos que utilizan los ciberdelincuentes para atacar a las personas (en muchos casos, los agresores combinan varias técnicas para eludir las defensas y aumentar su índice de éxito).

Ransomware

El ransomware, o secuestro de datos, es una antigua amenaza que sigue siendo un problema moderno. Este tipo de malware, que recibe su nombre del rescate (*ransom* en inglés) exigido para devolver a las víctimas el acceso a sus archivos, es un problema grave para todas las empresas. En la actualidad constituye uno de los tipos de ciberataque más destructivos.

Los principales incidentes que tuvieron lugar en 2021 afectaron al suministro de combustible[7], la alimentación[8] y la infraestructura sanitaria[9], lo que demuestra que no hay objetivos intocables.

Aproximadamente tres cuartas partes del ransomware se inician directa o indirectamente con un mensaje de phishing[10]. Estos mensajes incitan a los usuarios a abrir un adjunto malicioso o a hacer clic en una URL maliciosa.

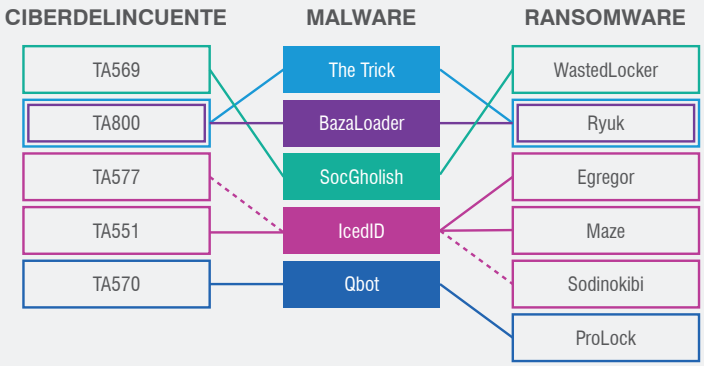


Figura 2: Relaciones entre los ciberdelincuentes, el malware de primera fase y el ransomware

En su mayoría, el ransomware se distribuye como infección secundaria una vez contaminado el sistema con un troyano o un cargador. A continuación, muchos ciberdelincuentes especializados en estos troyanos o cargadores venden el acceso a grupos de ransomware. Para la mayor parte de las organizaciones, la primera línea de defensa contra el ransomware es asegurarse de estar protegidas frente a otras clases de malware.

No hay una correspondencia directa entre el malware de acceso inicial y la variante de ransomware que se distribuye a las víctimas, pero los investigadores de Proofpoint y de otras empresas del sector han encontrado asociaciones importantes, como muestra la Figura 2.

7 David E. Sanger, Clifford Krauss, Nicole Perlroth (New York Times) "Cyberattack Forces a Shutdown of a Top U.S. Pipeline" (Un ciberataque obliga a cerrar un importante oleoducto estadounidense), mayo de 2021.
8 Julie Creswell, Nicole Perlroth, Noam Schreiber (New York Times) "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business" (Un ransomware paraliza las plantas de procesamiento cárnico en el último ataque a empresas fundamentales de EE. UU.), junio de 2021.
9 Nicole Perlroth, Adam Satariano (New York Times) "Irish Hospitals Are Latest to Be Hit by Ransomware Attacks" (Los hospitales irlandeses, últimos objetivos de los ataques de ransomware), mayo de 2021.
10 Unit 42, Palo Alto Networks. "Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report" (Familias de ransomware: datos de 2021 para complementar el informe sobre amenazas de ransomware de la Unit 42), julio de 2021.

Estafa por correo electrónico o Business Email Compromise (BEC)

Las estafas Business Email Compromise (BEC), también conocidas como estafas o fraude por correo electrónico, son una de las amenazas de ciberseguridad más costosas y menos conocidas. Se trata sin duda de un método que ha evolucionado rápidamente y que no siempre capta tanta atención como otros ciberdelitos más notorios. Sin embargo, en costes económicos directos, las estafas BEC eclipsan fácilmente a otros tipos de fraude.

Solo en 2020, los ataques BEC costaron a organizaciones y particulares más de 1800 millones de dólares[11], cifra que supera en más de 100 millones la de 2019 y que representa el 44 % de las pérdidas totales por ciberdelincuencia.

Los ataques BEC son difíciles de detectar. No incluyen las habituales payloads (URL o adjuntos de correo maliciosos) que permitan su análisis. En lugar de eso, los estafadores recurren a la suplantación de la identidad u otras técnicas de ingeniería social para engañar a las personas.

Muchos de los ataques BEC actuales son enormemente sofisticados, cuentan con una buena financiación y están cuidadosamente planificados y estudiados. Cada vez son más los ciberdelincuentes que centran sus esfuerzos en el fraude de facturas de proveedores y las grandes transacciones entre empresas (B2B) que pueden desviar a sus propias cuentas bancarias.

Los ataques BEC sacan partido de la naturaleza humana. Se aprovechan de la confianza de las personas.

Este es su *modus operandi*:

1. En primer lugar, los atacantes se hacen pasar por una persona o entidad de confianza de un destinatario, como un compañero de trabajo, su jefe o un proveedor.
2. El estafador envía un mensaje de correo electrónico al destinatario para conseguir apropiarse de dinero o de información financiera confidencial de la organización: transferencias bancarias fraudulentas, facturas falsas, desvío de nóminas, cambios en los detalles bancarios para futuros pagos y una innumerable lista de otros métodos fraudulentos.
3. Cuando la organización detecta el error, a menudo es demasiado tarde para recuperar el dinero.

TIPOS DE ATAQUES BEC

Los ataques BEC adoptan numerosas formas y solo están limitados por la creatividad de los ciberdelincuentes. Estos son seis ejemplos habituales:

1. **Fraude de facturas.** Este ataque engaña a las víctimas para que paguen facturas falsas o desvíen un pago válido.
2. **Desvío de nóminas.** Con este método, los ciberdelincuentes se hacen pasar por un empleado y piden al departamento de nóminas que redirija los sueldos a su cuenta.
3. **Extorsión.** Aquí los atacantes amenazan con dañar o humillar a la víctima si no paga.
4. **Señuelos y tareas.** Atraen a las víctimas con algo tan simple como "¿Estás ahí?" y pasan a otras formas de BEC.
5. **Tarjetas regalo.** Esta técnica induce al destinatario a comprar tarjetas regalo y a enviar el número de las tarjetas y el PIN al estafador.
6. **Fraude de los anticipos.** En esta vieja estafa, los timadores piden dinero para liberar una suma incluso mayor que nunca llega.

11 FBI. "Internet Crime Report 2020" (Informe sobre delitos en Internet de 2020), marzo de 2021.

Compromiso/usurpación de cuentas

El compromiso de cuentas consiste en hacerse con el control de la cuenta de un servicio de correo web o cloud legítimo con el fin de acceder a una amplia variedad de datos, contactos, eventos de calendario y mensajes de correo electrónico.

Aparte de los datos del usuario comprometido, el ciberdelincuente puede utilizar la cuenta para suplantar su identidad en ataques de ingeniería social, tanto dentro como fuera de la organización, incluidos ataques BEC, ataques a la cadena de suministro y otros.

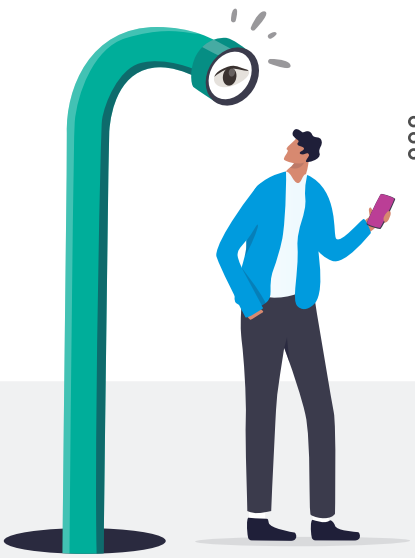
Los ciberdelincuentes pueden acceder a datos sensibles, persuadir a los usuarios o a partners comerciales a transferir dinero o dañar la reputación y la economía de una empresa. Peor aún, también pueden instalar puertas traseras para conservar el acceso para futuros ataques.

Anatomía de una usurpación de cuentas cloud

A continuación detallamos el desarrollo de la mayoría de las usurpaciones de cuentas.

Robo de credenciales. El ciberdelincuente consigue las credenciales del usuario a través de phishing de credenciales (que por sí solo constituye cerca de dos tercios de todo el volumen de phishing), ataques de contraseña por fuerza bruta, reciclado o stuffing de credenciales o malware de robo de credenciales.

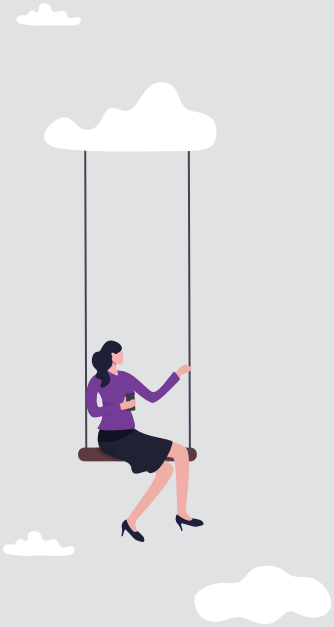
Infiltración. Una vez conectado a la cuenta del usuario, el ciberdelincuente puede acceder a los mensajes de correo, a los contactos, al calendario y a los archivos de la víctima. Entonces puede robar directamente esos datos o utilizarlos para suplantar la identidad del usuario de una manera convincente. Algunos estafadores responden a hilos de discusión existentes o envían mensajes de correo electrónico que contienen malware o URL peligrosas a compañeros y a partners comerciales externos. Otros, haciéndose pasar por el usuario comprometido, pueden engañar a otras personas dentro o fuera de la empresa enviándoles facturas falsas o instrucciones de desvío de pagos. También pueden cargar malware en recursos compartidos de archivos corporativos o sabotear la empresa de otras maneras.



Persistencia. A menudo, el ciberdelincuente define subrepticiamente reglas de reenvío automático que le permiten acceder a los mensajes del usuario incluso si este cambia su contraseña. Al ser capaz de acceder a todos sus mensajes de correo electrónico e invitaciones de calendario, el ciberdelincuente obtiene información esencial para futuros ataques de suplantación.

SECCIÓN 2

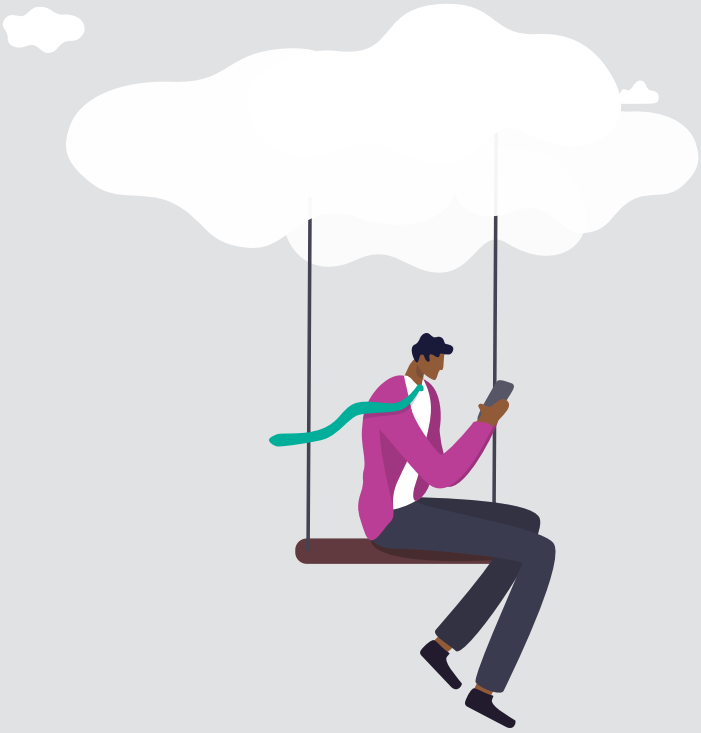
Evolución del panorama de amenazas

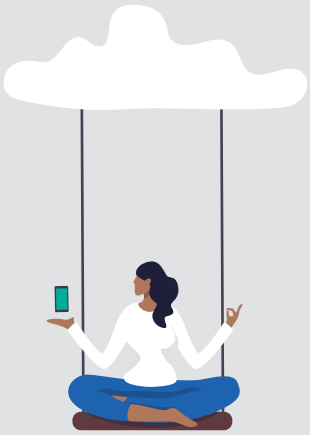


Los modelos actuales de trabajo remoto e híbrido funcionan con tecnologías cloud y móviles.

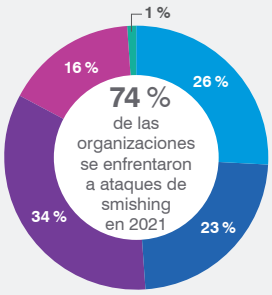
Los perímetros reforzados y las estructuras de red tradicionales son cosa del pasado. El nuevo perímetro son las personas.

Lamentablemente, la mayoría de los presupuestos de seguridad, pendientes también de otras prioridades y categorías de productos, no han podido adaptarse.

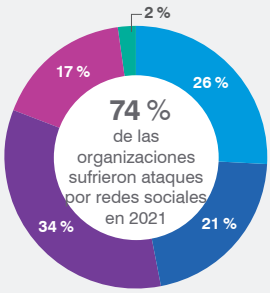




Volumen de ataques de smishing

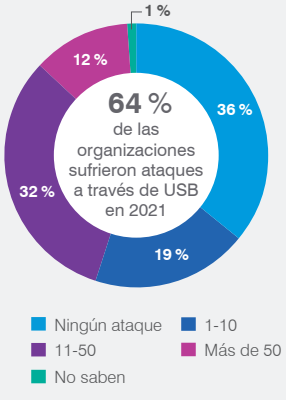


Volumen de ataques por redes sociales



Volumen de vishing

Volumen de ataques por dispositivos USB con malware



Fuente: Informe State of the Phish 2022

El objetivo de los ciberdelincuentes son las personas, no la infraestructura

Aunque las organizaciones invierten miles de millones al año en reforzar su infraestructura, a veces olvidan los riesgos de seguridad más importantes: los que generan las personas. Ellas son el punto de entrada más fácil y lucrativo al entorno.

Según el informe de Verizon sobre las investigaciones de fugas de datos, hasta un 85 % de las fugas de datos implican la intervención humana[12]. Los usuarios se enfrentan a un constante aluvión de hiperenlaces no seguros, robo de credenciales, tácticas de ingeniería social y amenazas de impostores.

Los ataques suelen cubrir múltiples vectores

Para atacar a las personas, es preciso interaccionar con ellas en las herramientas y las plataformas que utilizan. Los ciberdelincuentes siguen a las personas, allí donde estas van.

Los flujos de trabajo actuales son dinámicos e imprevisibles. Un usuario puede iniciar una conversación por correo electrónico, concertar una reunión de seguimiento en la aplicación de chat y colaborar en archivos guardados en servicios cloud.

También los ataques modernos son dinámicos e impredecibles. Se perpetran en múltiples canales, combinan diferentes tácticas y herramientas y aprovechan todas las plataformas que utilizan las personas para hacer su trabajo.

Un ataque puede iniciarse con un mensaje de correo electrónico que dirige a un malware alojado en un sitio de uso compartido de archivos. Pero también puede adoptar la forma de una aplicación cloud no autorizada y así robar credenciales, comprometer una cuenta legítima y utilizarla para lanzar ataques BEC.

El reto no hace más que crecer. A menudo, un autor de amenazas avanzadas crea un "producto" de malware y configura la infraestructura como paquete o servicio fácil de utilizar. Los ciberdelincuentes de niveles inferiores pueden alquilar el servicio para sus ataques, pagar por usarlo durante un período de tiempo determinado o conseguir una parte por cada ofensiva de éxito. En otros casos, actúan como distribuidores, envían mensajes de correo electrónico con el malware y ganan una comisión por cada infección.

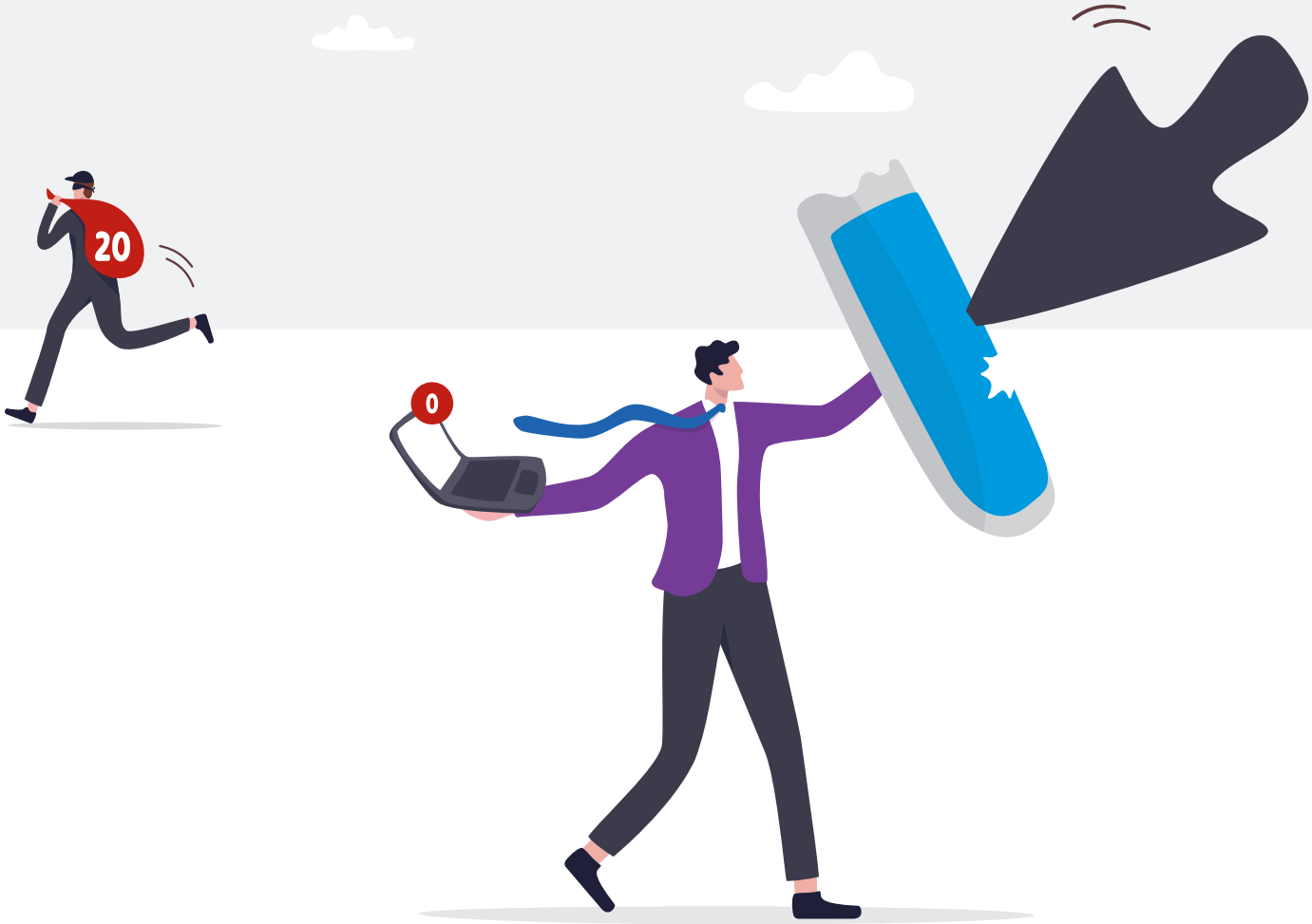
12 Verizon. "Data Breach Investigations Report" (Informe de investigaciones de fugas de datos - Resumen ejecutivo), mayo de 2021.

No basta con proteger todos los vectores

Hay organizaciones que saben que las amenazas actuales tienen múltiples facetas y que están principalmente dirigidas a las personas, y por ello invierten en herramientas de seguridad que cubran todos los riesgos potenciales. Pero si estas herramientas no funcionan conjuntamente de forma coordinada, no pueden ofrecer la visibilidad y la información que los equipos de seguridad necesitan para gestionar los riesgos.

Imaginemos un equipo de estrellas de fútbol que entrenan por separado, una orquesta de virtuosos que ensayan sin los demás instrumentos o un equipo quirúrgico que no se pone de acuerdo sobre el tratamiento de un paciente. Por competente que sea cada persona, nunca serán tan eficaces como un grupo bien coordinado.

Actualmente, los ciberdelincuentes combinan diversas técnicas para que sus ataques sean más sofisticados. Las herramientas aisladas complican innecesariamente la labor de unos equipos de seguridad que ya tienen dificultades para enfrentarse a los riesgos actuales. Por ello, una seguridad verdaderamente centrada en las personas requiere un enfoque integral y coordinado.



SECCIÓN 3

Céntrese en los empleados de mayor riesgo

El primer paso para proteger a los usuarios es identificar a aquellos que suponen un mayor riesgo. Si bien cada organización puede sopesar de forma diferente los distintos factores de riesgo, todas las estrategias deberían incluir al menos una combinación de los siguientes: vulnerabilidad, ataques y privilegios.

La vulnerabilidad es la forma de determinar quién tiene más probabilidad de convertirse en víctima de una amenaza. Un análisis de los ataques puede revelar quién en la organización está sufriendo ataques, la intensidad de los mismos y con qué tipos de amenazas. Los privilegios ayudan a predecir el nivel de daños que producirá un ataque en una organización si consigue su objetivo.

Basándose en cualquier combinación de estos factores, céntrese en los usuarios que representan un riesgo superior a lo normal. El equipo de seguridad y las partes interesadas deben prestarles más atención para averiguar cómo y por qué corren peligro.

Este nivel de visibilidad en estas tres áreas es esencial para impulsar una estrategia de seguridad centrada en las personas. Sin ella, las organizaciones no pueden saber quién necesita más seguridad o cómo se les puede proteger mejor.

Vulnerabilidad: cómo trabajan los empleados y dónde hacen clic

Cuantificar el grado de vulnerabilidad no es una tarea fácil con herramientas de seguridad centradas en la tecnología. Pero con un enfoque centrado en las personas, se puede medir cómo trabajan los empleados y en qué hacen clic.

Su modo de trabajo incluye las herramientas, sistemas y plataformas que emplean. Saber dónde hacen clic es una medida de su nivel de concienciación en materia de seguridad y de su propensión a caer en la trampa de posibles amenazas.

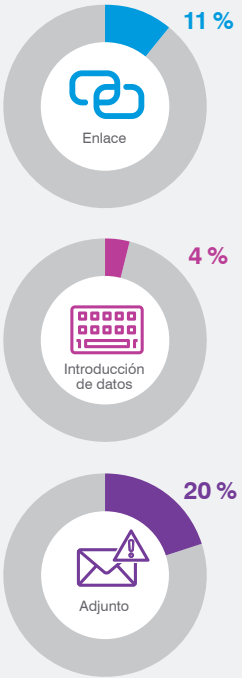
Cómo trabajan sus empleados

Puede hacerse una idea general de la vulnerabilidad de los usuarios evaluando qué herramientas, plataformas y aplicaciones utilizan. Por ejemplo:

- Qué aplicaciones cloud emplean y si las ha autorizado el departamento de TI.
- Cuántos dispositivos usan para acceder al correo electrónico y cuáles son.
- Si son seguros dichos dispositivos.
- Si los usuarios mantienen buenos hábitos digitales, como el uso de contraseñas seguras y únicas y la puntual actualización del software.
- Si utilizan siempre autenticación multifactor para acceder a las cuentas empresariales e incluso personales.

Cuanto mayor y más granular sea la visibilidad, mejor.

Tipos de plantillas de phishing: tasas medias de fallos



Fuente: Informe State of the Phish 2022

Dónde hacen clic sus empleados

La vulnerabilidad puede medirse con más precisión mediante formación en seguridad, simulaciones de phishing y análisis de la reacción ante amenazas reales.

La formación para concienciar en materia de seguridad, un componente esencial de toda estrategia de seguridad eficaz, ofrece información sobre qué usuarios están menos preparados para reconocer, resistir y denunciar ciberamenazas. En general, los usuarios que obtienen una puntuación baja en los ejercicios de formación, o que no los han realizado, son más vulnerables que los que tienen puntuaciones más altas.

Descartada la posibilidad de permitir el acceso a los atacantes para descubrir quién hace clic en un enlace, rellena un formulario o abre un archivo, las simulaciones de phishing son una de las formas más eficaces de evaluar este aspecto de la vulnerabilidad.

Por último, lo más importante es llevar un seguimiento de los usuarios que interaccionan con mensajes maliciosos conocidos, incluso cuando el clic se bloquea, aísla o reescribe.

Estos datos reales, combinados con información de concienciación en materia de seguridad, ofrecen una visión global de la vulnerabilidad del correo electrónico gracias al seguimiento de los cursos realizados, las simulaciones de phishing y la interacción con mensajes maliciosos reales.

Ataques: cómo determinan sus objetivos

Todo ciberataque es dañino en potencia. Sin embargo, algunos son más peligrosos, dirigidos o sofisticados que otros. Por eso medir este aspecto del riesgo puede ser más complicado de lo que parece.

Probablemente las amenazas indiscriminadas de bajo perfil son las más numerosas. Pero se conocen bien y se bloquean más fácilmente.

En cambio, hay otras amenazas que aparecen solo en contados ataques y que, por su nivel de sofisticación o las personas a las que van dirigidas, son más peligrosas.

Conocer la diferencia es esencial para identificar a los usuarios que están expuestos a un mayor riesgo. En Proofpoint, a estos usuarios los llamamos VAP (Very Attacked People™, o personas muy atacadas). La visibilidad completa de todo el tráfico del correo electrónico, acompañada de una inteligencia de amenazas detallada, son claves para cuantificar quién recibe ataques y con qué intensidad.

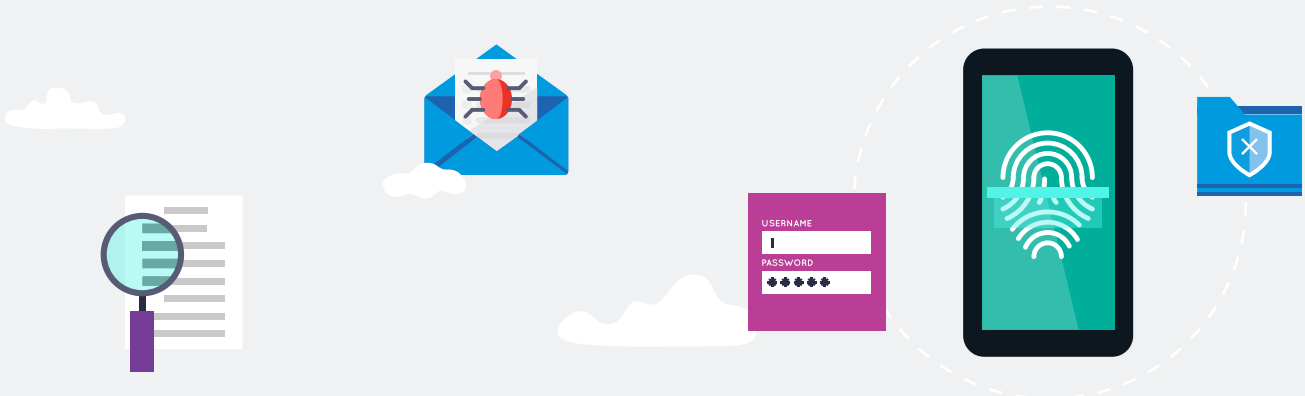
Entre los factores que más deben influir en la evaluación de cada usuario se incluyen:

- El nivel de sofisticación del ciberdelincuente
- El alcance y objetivo de los ataques
- El tipo de ataque
- El volumen global de ataques

También se deben tener en cuenta estos factores en el contexto de los departamentos, grupos o divisiones a los que pertenece el usuario.

Por ejemplo, podría parecer que algunos usuarios no representan un riesgo, dado el volumen o el tipo de mensajes maliciosos que reciben directamente. Sin embargo, el riesgo puede ser mayor si se tiene en cuenta que trabajan en un departamento muy atacado y, por lo tanto, tienen más probabilidades de ser un objetivo clave en el futuro.

Una buena inteligencia sobre amenazas puede averiguar qué herramientas utilizan los agresores y asociar incidentes aparentemente aislados a campañas de mayor envergadura.



Privilegios: a qué tienen acceso los empleados

Para medir los privilegios de los usuarios se debe hacer un inventario de todos los recursos potencialmente valiosos a los que tienen acceso: datos, autoridad financiera, relaciones estratégicas, etc. Es preciso saber dónde se encuentran los datos más sensibles y qué usuarios o aplicaciones acceden a ellos.

Los usuarios con acceso a sistemas críticos o propiedad intelectual, por ejemplo, pueden necesitar protección adicional, incluso aunque no sean especialmente vulnerables o no estén aún en el punto de mira de los ciberdelincuentes.

Lógicamente, el cargo del empleado en la empresa es un factor que cuenta a la hora de determinar y calificar sus privilegios. Pero no es el único y, con frecuencia, ni siquiera es el más importante.

Un asistente de dirección puede ser más atractivo para un espía que un mando intermedio, ya que el asistente tiene acceso al calendario del CEO. De la misma forma, una enfermera de un hospital con acceso a las historias clínicas de los pacientes puede ser un objetivo más útil para los ladrones de identidades que el CEO.

Para los agresores, un objetivo valioso será cualquiera que les sirva como medio para conseguir su fin.

Tan fundamental es proteger de ataques externos a los usuarios con privilegios elevados como proteger de estos usuarios a la organización. En las manos equivocadas, el acceso interno puede utilizarse indebidamente, ya sea por negligencia, de forma maliciosa o para comprometer una cuenta. Las cuentas comprometidas pueden servir para exportar archivos confidenciales o intentar comprometer o engañar a otros usuarios internos.

SECCIÓN 4

Construcción de una defensa centrada en las personas

Un enfoque centrado en las personas garantiza la protección de todos, ya que aplica los controles de seguridad adecuados para sus niveles de riesgo. Y funciona de forma unificada en todas las plataformas utilizadas, contra todas las tácticas que emplean los ciberdelincuentes y en todos los vectores de amenaza importantes.

Nivel básico: seguridad para todos

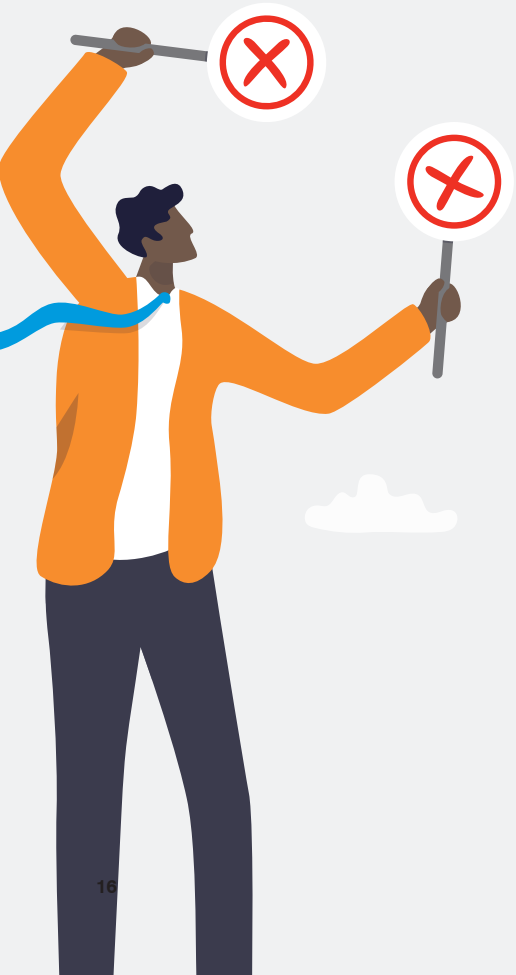
Los ataques por correo electrónico llegan de muchas formas, por lo que necesita una defensa que detenga toda la gama de amenazas, no solo algunas.

Estos son los pasos más importantes para construir una defensa del correo electrónico diseñada para las amenazas actuales:

- Neutralizar adjuntos y URL maliciosos antes de que lleguen a la bandeja de entrada de los usuarios.
- Neutralizar los ataques de impostores que no utilizan payloads, como los ataques BEC y otros timos, incluidas las procedentes de cuentas de correo electrónico comprometidas dentro de su propia organización y de los proveedores.
- Proteger la navegación web y el correo electrónico personal del usuario con aislamiento web y de correo electrónico personal.
- Conseguir que los usuarios sean más resilientes con formación para concienciar en materia de seguridad e información contextual.
- Aplicar controles tales como el aislamiento web para aislar del entorno los hábitos de navegación potencialmente inseguros de los usuarios.
- Incluir la protección de datos en la estrategia de seguridad del correo electrónico.

Neutralizar adjuntos y URL maliciosos antes de que lleguen a la bandeja de entrada de los usuarios.

La mayoría de los ciberataques dependen de que la víctima realice alguna acción, en muchos casos, abrir un archivo adjunto o hacer clic en una dirección URL. Pero los ataques que activan las personas no tendrán éxito si la víctima no llega nunca a ver el mensaje.



Y ahí entra en juego la protección de la seguridad del correo electrónico. Al bloquear las cargas maliciosas antes de que lleguen a la bandeja de entrada de los usuarios, una solución eficaz puede proteger frente a una amplia variedad de amenazas de malware, como el ransomware, los troyanos bancarios, los troyanos de acceso remoto, los ladrones de información, los descargadores o las redes de bots, entre otras.

Neutralizar los ataques de impostores difíciles de detectar.

Aunque neutralizar el malware es fundamental, algunos de los ataques por correo electrónico más dañinos no utilizan payloads, sino que emplean técnicas de ingeniería social.

Los ataques BEC, un tipo de estafa que usa las transferencias bancarias, son un ejemplo. Según el FBI, se han denunciado ataques BEC en 50 estados y 177 países, y se han enviado transferencias fraudulentas al menos a 140 países[13].

En los ataques BEC y en otras formas de fraude por correo electrónico, el timador se hace pasar por alguien en quien el destinatario confía, mediante una cuenta de correo falsificada, comprometida o similar a la auténtica. Con esa identidad falsa, el ciberdelincuente solicita a la víctima alguna acción, como transferir dinero a una cuenta bancaria en el extranjero o enviar archivos de carácter confidencial, por ejemplo.

Las amenazas de impostores son un problema complejo que tiene muchas vertientes. Para detenerlas, necesita una defensa por capas que proteja el correo entrante, saliente e interno, y que funcione de una forma holística y coherente.

13 FBI. "Internet Crime Report 2020" (Informe sobre delitos en Internet de 2020), marzo de 2021.

Junto a la formación de los usuarios y otros controles de seguridad descritos en este apartado, a continuación se incluyen los elementos clave para la defensa del correo electrónico de impostores.

DMARC

Despliegue el protocolo DMARC (Domain-based Message Authentication, Reporting and Conformance) para facilitar la autenticación de los mensajes de correo electrónico. DMARC es una política para todo internet que valida que el remitente del correo electrónico es quien dice ser y que está autorizado a enviar un mensaje en nombre de la organización.

DMARC ofrece visibilidad de todo el correo electrónico que se envía utilizando su dominio, incluido el caso de remitentes externos de confianza, como Marketo, Salesforce y otros. Con este nivel de visibilidad, puede autorizar a todos los remitentes válidos que intentan enviar mensajes en su nombre y bloquear a los que intenten usar sus dominios de confianza para robar dinero o dañar su imagen de marca.

Clasificación dinámica

DMARC puede ayudar a detener las amenazas que falsifican su dominio; sin embargo, los ciberdelincuentes recurren a otras técnicas para engañar a los usuarios. Por eso otro componente esencial para detener las amenazas que no emplean malware es analizar y clasificar de forma dinámica el contenido de los mensajes de correo electrónico. Este aspecto de la seguridad del correo electrónico consiste en analizar el contenido del mensaje, y no solo de dónde procede. Por ello, necesita una seguridad del correo electrónico que busque indicios reveladores de fraude y bloquee o investigue todo aquello que parezca poco seguro. La clasificación dinámica analiza y gestiona el correo electrónico basándose en varios factores, como:

- Encabezado del mensaje de correo electrónico, dirección IP y reputación del remitente
- Análisis de contenido mediante aprendizaje automático para detectar cambios de la dirección de respuesta y determinadas palabras o expresiones
- La relación entre el remitente y el destinatario
- Contexto sobre el remitente, como si parece suplantar a un proveedor conocido

Información sobre la protección del correo electrónico interno y el riesgo asociado a los proveedores

En algunos casos, los ciberdelincuentes ni siquiera disfrazan sus direcciones de correo electrónico, sino que se limitan a usurpar una cuenta legítima de la organización, un proveedor o un partner. El secuestro de cuentas de correo o compromiso de cuentas (EAC) se puede utilizar en muy distintos ataques, pero es especialmente eficaz como táctica de suplantación de identidad. Esto se debe a lo siguiente:

- La mayoría de las organizaciones no someten el correo interno al mismo nivel de escrutinio y control de seguridad que el correo externo.
- La mayoría de los usuarios confían por defecto en el correo electrónico que procede de personas que conocen.
- Los ciberdelincuentes que usurpan una cuenta disponen de abundante información sobre el usuario en peligro: con quién suele intercambiar mensajes, qué temas trata e incluso su estilo de redacción. Estos detalles consiguen que la suplantación de identidad sea particularmente convincente.

La protección de los usuarios internos y la recopilación del contexto sobre los riesgos asociados al proveedor son aspectos fundamentales para una seguridad eficaz del correo electrónico.

Conseguir que los usuarios sean más resilientes con formación para concienciar en materia de seguridad.

Los ciberdelincuentes se revelan como inexorablemente eficaces en sus intentos de aprovecharse de la naturaleza humana mediante el empleo de técnicas de falsificación convincentes, líneas de asunto que captan la atención y llamadas a la acción difíciles de resistir. En un gran número de casos, los destinatarios no son los únicos en hacer clic, ya que el mensaje se reenvía a otras personas que también caen en la trampa.

La formación para concienciar en materia de seguridad, especialmente como pilar de una cultura de seguridad generalizada, puede ser de gran ayuda para convertir a los usuarios en una última línea de defensa sólida. Pero, para resultar eficaz entre los usuarios, debe estar personalizada, ser constante e impartirse siempre que convenga. Un curso genérico anual no basta para modificar comportamientos ni crear una cultura de seguridad.

Las etiquetas del correo electrónico que brindan a los usuarios información contextual sobre la naturaleza del mensaje también pueden ayudarles a localizar y denunciar posibles amenazas. Por ejemplo, una etiqueta que informe al usuario de que el mensaje procede de una dirección externa o de que el dominio de correo electrónico es extrañamente similar al de una marca de confianza puede ayudarle a detectar un posible intento de phishing.

El aislamiento web y del correo electrónico es otro control que puede aplicarse para confinar y analizar automáticamente los clics en mensajes que puedan conducir a sitios falsos de inicio de sesión con credenciales, abrir adjuntos o URL maliciosos que contengan malware, u otras amenazas. Todo ello puede aplicarse a los usuarios de mayor riesgo, los VIP o una base de usuarios más amplia en función del riesgo.

15,4 M$

en daños por organización en 2021.

Proteger frente a la fuga de datos y amenazas internas.

No hay defensa del correo electrónico capaz de detener todas las amenazas. Y ni siquiera los empleados con mejor formación se libran de caer en la trampa de los ataques más dirigidos, que emplean tácticas de ingeniería social.

Por este motivo, toda defensa del correo electrónico debe incluir herramientas de prevención de la pérdida de datos (DLP), como el cifrado. Incluso si algo falla, con una respuesta rápida y una herramienta de DLP se puede garantizar que el ataque no se propague y que los ciberdelincuentes no consigan sus datos más confidenciales.

La prevención de pérdida de datos es también una defensa útil frente a las amenazas internas. A nadie le gusta considerar a su compañero como un potencial enemigo de la seguridad. Pero las amenazas internas —ya sea a causa de empleados poco cautos, malintencionados o con cuentas comprometidas— provocaron de media 15,4 millones de dólares en daños por organización en 2021[14].

Tanto ante fugas externas de datos como frente a ataques internos, DLP le ayuda a mantener los datos de su entorno protegidos.

14 Ponemon Institute. "2022 Cost of Insider Threats Global Report" (Informe de 2022 sobre el coste de las amenazas internas a nivel mundial), enero de 2022.

Nivel adaptable: controles adaptables para los usuarios de más riesgo

Una protección centrada en las personas bien perfilada reconoce que hay usuarios que necesitan niveles de seguridad y controles adicionales. Estos usuarios pueden ser más propensos a convertirse en víctimas, recibir más ataques o tener privilegios más elevados sobre sistemas y datos confidenciales. O bien puede darse una combinación de estos tres factores que determine que su riego general sea más alto.

Los siguientes controles son esenciales para los usuarios de mayor riesgo:

- Formación dirigida para concienciar en materia de seguridad.
- Protecciones adaptables, basadas en el riesgo, como la autenticación y el aislamiento web y de URL.
- Protección frente al compromiso de cuentas cloud.

Formación dirigida para concienciar en materia de seguridad

La formación para concienciar en materia de seguridad para toda la empresa es útil para revelar las vulnerabilidades y reducir la superficie de ataque a personas. Además de solventar vacíos de conocimiento evidentes, la formación dirigida o focalizada también es una medida de prevención eficaz para todos los usuarios de riesgo, no solo para los que tienen un alto nivel de vulnerabilidad.

Los usuarios que suponen más riesgo debido a su perfil de ataque, por ejemplo, pueden adquirir formación sobre las amenazas concretas que les afectan a ellos. Y los usuarios con privilegios elevados pueden obtener formación adicional en relación con las campañas de ataque contra los datos a los que ellos tienen acceso.

Controles adaptables y basados en el riesgo

En la mayoría de las organizaciones, aplicar los controles de seguridad más estrictos a todos los usuarios todo el tiempo no es práctico. Puede ser contraproducente. Los controles innecesariamente severos pueden afectar a la productividad de los usuarios y llevarles a sortear la seguridad para poder hacer su trabajo.

Sin embargo, en ocasiones, se necesita esa capa adicional de seguridad. Un empleado que trabaja en primera línea puede ser más propenso a recibir un ataque. Un investigador puede ser víctima de un ciberdelincuente especialmente sofisticado. O un CEO, debido a la naturaleza de su trabajo, puede tener acceso a los datos más sensibles de la empresa.

En algunas ocasiones, quizá sea necesario reforzar los requisitos de autenticación. En otros casos, es posible que necesite aislamiento web para las URL en las que el usuario hace clic en un mensaje de correo electrónico.

Sea cual fuere la forma que adopte, la protección adaptable requiere disponer de una imagen puntual de los factores de riesgo relativos a los VAP y aplicar controles que sean proporcionales a dicho riesgo.

Protecciones de cuentas cloud

Para un ciberdelincuente, una cuenta comprometida es prácticamente como una licencia para robar.

Una cuenta comprometida se puede utilizar de infinidad de formas con fines maliciosos. Si consigue el control de acceso del usuario adecuado, el intruso se puede desplazar lateralmente dentro del entorno, robar datos o timar a sus partners y clientes. Por eso, proteger las cuentas de correo electrónico, particularmente las cuentas cloud, es fundamental.

Nivel de respuesta: detención de amenazas más rápida y eficaz

Si bien es cierto que los incidentes de seguridad son inevitables, no tienen por qué ser catastróficos.

Cuando un ataque consigue superar las defensas, la rapidez con la que se contengan y reparen los daños puede marcar la diferencia entre un incidente puntual y un problema de largo alcance. Por eso, una plataforma de respuesta sólida es una parte fundamental de toda iniciativa de seguridad centrada en las personas.

En muchas empresas, la respuesta ante los incidentes de seguridad es un proceso lento y laborioso que incluye:

- Investigación y verificación del incidente
- Cuarentena de mensajes de correo electrónico no seguros
- Contención de la amenaza
- Determinación de la causa y el alcance
- Corrección de los sistemas infectados

Todos estos pasos son esenciales para que la respuesta sea eficaz. Pero como bien saben los responsables de seguridad, si se llevan a cabo de forma manual no se pueden escalar. Y aquí es donde puede ayudar la automatización.

Los procesos de respuesta eficaces automatizan tareas que requieren mucho trabajo, como la correlación y el análisis de las alertas de seguridad, la verificación de indicadores de compromiso y la recopilación de datos forenses. Además, la automatización puede ayudar en las tareas de remediación, como la actualización de firewalls y listas de bloqueo del correo electrónico, la extracción de mensajes maliciosos de las bandejas de entrada y la restricción de acceso a las cuentas de los usuarios afectados.

Cuando se utiliza estratégicamente, la automatización agiliza la respuesta a incidentes y libera a su personal de seguridad para que dedique su tiempo a las tareas que las personas hacemos mejor. En lugar de reaccionar a multitud de amenazas, pueden aplicar medidas de protección proactivas.

Cómo ayudan la inteligencia artificial y el aprendizaje automático

El objetivo de los ciberdelincuentes son las personas. Su meta es aprovecharse de la gente. Después de todo, ellos mismos son personas.

Para detenerles, se precisan soluciones modernas que puedan adaptarse al comportamiento humano. Por eso, el aprendizaje automático es un componente fundamental de cualquier estrategia de seguridad centrada en las personas.

El aprendizaje automático es más ágil y eficaz que el análisis humano manual. Y, a diferencia de los algoritmos tradicionales basados en reglas, puede adaptarse rápidamente a las nuevas y cambiantes amenazas y tendencias.

El aprendizaje automático en la lucha contra los ataques BEC

Veamos el ejemplo de las estafas BEC. Los ataques BEC de facturas a proveedores son tácticas sofisticadas y complejas que tienen como objetivo el robo de dinero. Consisten en presentar una factura fraudulenta como legítima o desviar un pago a una cuenta bancaria controlada por el ciberdelincuente.

Las herramientas de seguridad tradicionales no logran neutralizar este tipo de ataques por un doble motivo: están altamente dirigidos y no contienen payloads. El aprendizaje automático puede analizar dinámicamente una amplia variedad de atributos de mensaje —incluida la información del encabezado, el dominio y el cuerpo del mensaje— para detectar el mensaje de un impostor o un proveedor comprometido.

Análisis del phishing de credenciales

Tenemos otro ejemplo en los ataques de phishing de credenciales. Estos ataques de ingeniería social suelen utilizar sitios de inicio de sesión falsos para conseguir que las víctimas introduzcan sus credenciales. Normalmente están tan bien diseñados que los usuarios no pueden distinguirlos a simple vista. Sin embargo, con el uso del aprendizaje automático y la visión artificial para analizar rápidamente las URL, las herramientas de seguridad modernas pueden detectar y bloquear todos los mensajes que redirigen a sitios falsos. El aprendizaje automático es capaz de detectar las URL peligrosas, incluso si están recién registradas, se alojan en sitios de uso compartido de archivos o utilizan técnicas de evasión avanzadas como CAPTCHA.

Basura que entra y sale (GIGO)

A diferencia de los sistemas de software estándar basados en reglas, el comportamiento del aprendizaje automático se basa en datos y no se codifica manualmente. Esto significa que la calidad de los sistemas de aprendizaje automático depende de las personas que los entrenan y de los datos que utilizan.

A la hora de evaluar a los proveedores que ofrecen funciones de aprendizaje automático, busque modelos entrenados con grandes conjuntos de datos de amenazas. Estos datos deben incluir información de amenazas procedente de empresas destacadas que figuren en las listas Fortune 100, Fortune 1000 y Fortune Global 2000, así como del mayor número posible de proveedores de servicios de Internet y pymes. Y debe abarcar múltiples vectores de ataque, como el correo electrónico, la nube, la red y las redes sociales. Estos canales son imprescindibles, ya que los ciberdelincuentes despliegan su arsenal más allá del correo electrónico.

Y no olvide el papel de los investigadores de amenazas cualificados para entrenar los modelos de aprendizaje automático. Por sí solos, ni los mejores científicos de datos pueden crear un modelo de aprendizaje automático eficaz. Necesitan la experiencia práctica que acompaña a un amplio bagaje en investigación y análisis de amenazas.

LISTA DE VERIFICACIÓN

Funciones indispensables de una solución de seguridad

La seguridad centrada en las personas no es un mero eslogan publicitario, sino una forma radicalmente nueva de considerar las amenazas y cómo detenerlas. Se basa en la estrategia adecuada, pero también exige utilizar las herramientas y las funciones correctas.

A continuación, se incluye una lista de qué hay que pedirle a una solución de seguridad centrada en las personas.

Una plataforma unificada, integrada y escalable

Una solución de seguridad centrada en las personas es algo más que la suma de sus partes. Las soluciones aisladas pueden resolver algunos aspectos de su problema de seguridad, pero, para combatir las amenazas modernas, hace falta una estrategia integral que aborde todas las tácticas, herramientas y vectores que emplean los ciberdelincuentes, y en todos los dispositivos, plataformas y canales que utilizan sus empleados.

El uso de productos de seguridad no integrados que requieren varias consolas hace que se pierdan tiempo y recursos en flujos de trabajo repetidos y complicados. Los equipos de seguridad tienen una visión fragmentada de las amenazas, una carga de trabajo innecesaria y una excesiva complejidad de administración.

Busque soluciones que cubran una amplia variedad de amenazas y que se integren en su ecosistema de seguridad. Dependiendo de su organización, estas pueden incluir componentes tales como firewalls de nueva generación, sistemas de administración de información y eventos de seguridad (SIEM) y herramientas de gestión de identidades.

Protección eficaz para todos los usuarios

La mejor manera de neutralizar los ataques por correo electrónico es adoptar una estrategia multicapa, como hace tiempo recomiendan Gartner y otros expertos.

Asegúrese de que sus ciberdefensas puedan mitigar:

- Spam y correo electrónico no deseado masivo.
- Ataques que utilizan adjuntos y URL maliciosos.
- Ataques que no utilizan payloads, como los BEC.
- Compromiso de cuentas de correo electrónico y usurpación de cuentas cloud.

Las personas desempeñan un papel clave en los ataques de correo electrónico. Por eso la formación para concienciar en materia de seguridad es fundamental en su estrategia de seguridad del correo electrónico. Asegúrese de que su programa de formación incluya lo siguiente:

- Píldoras formativas que aseguren la participación y promuevan cambios de comportamiento.
- Simulaciones de phishing basadas en campañas del mundo real que sirvan para formar a los usuarios sobre las amenazas a las que con mayor probabilidad se van a enfrentar.
- Cursos periódicos basados en datos para los usuarios vulnerables que reciban ataques o interaccionen con mensajes de phishing reales.
- Etiquetas de correo electrónico que alerten a los usuarios para que tengan cuidado con los mensajes sospechosos, con mecanismos de denuncia incorporados e información sobre el resultado de la denuncia.

Para proteger los datos que un empleado interno ha robado, compartido por error o expuesto con fines malintencionados, el cifrado y otras medidas de DLP son esenciales. Una herramienta de DLP eficaz puede:

- Analizar y clasificar el contenido en detalle y, cuando sea necesario, bloquearlo para impedir su envío por correo electrónico, su transferencia a la nube o su carga en un dispositivo USB.
- Identificar a los usuarios maliciosos, negligentes o víctimas de un ataque y ayudar a los equipos de TI, RR. HH., servicios jurídicos y seguridad a tomar las medidas adecuadas para evitar daños permanentes.
- Identificar y proteger todas las formas estándar de contenido restringido, como el regulado por normativas, como PCI, HIPAA, FINRA y otras.
- Redirigir, cifrar o rechazar automáticamente los mensajes que infrinjan las normativas de seguridad o de otro tipo, y alertar a las personas adecuadas dentro de su empresa.

Controles adaptables para los usuarios de más riesgo

Los usuarios de alto riesgo —en función de su vulnerabilidad, su perfil de ataque y sus privilegios— requieren controles de seguridad adicionales. Una solución de seguridad del correo electrónico centrada en las personas le ayuda a identificar a esos VAP y a protegerlos con capas de seguridad adicionales. Busque una solución que:

- Le proporcione visibilidad de sus VAP, con inteligencia de amenazas detallada y puntual, así como una visión profunda de los perfiles de riesgo de los usuarios.
- Ofrezca herramientas de generación de informes que faciliten la detección y comunicación de la vulnerabilidad, el perfil de ataque y los privilegios de los empleados, con comparaciones entre departamentos y sectores.
- Responda automáticamente a cambios en los perfiles de riesgo de los usuarios con una autenticación más estricta, una reducción de los privilegios y el aislamiento de URL, entre otras medidas.

Respuesta rápida y eficaz cuando algo consigue acceder

La automatización de partes clave del proceso de respuesta a incidentes puede simplificar tareas laboriosas que son esenciales y liberar a los responsables de la respuesta para que se encarguen de tareas de más alto nivel. Busque herramientas de respuesta automatizada que:

- Verifiquen las amenazas, identifiquen a los usuarios afectados y recopilen datos forenses y contexto sobre dichos usuarios.
- Enriquezcan las alertas de amenazas con inteligencia práctica.
- Contengan y corrijan las amenazas en todo el entorno, ya sea en la nube o de forma local. Las medidas correctivas automatizadas pueden incluir el análisis de los mensajes denunciados por los usuarios, la extracción de las amenazas verificadas de la bandeja de entrada del usuario y el restablecimiento de contraseñas en las cuentas comprometidas.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 75 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en www.**proofpoint.com/es**.

proofpoint.

0301-001-01-03 03/22