Octubre de 2025

Informe de mercado

Informe sobre brechas de seguridad del correo electrónico 2025

La experiencia e impacto de las brechas de seguridad del correo electrónico en organizaciones de todo el mundo

Barracuda®
Your business, secured.

Contenido

Introducción

Este informe explora la experiencia y el impacto de las brechas de seguridad del correo electrónico en organizaciones de todo el mundo en los últimos 12 meses. Se basa en los hallazgos de una encuesta internacional realizada a 2,000 responsables de decisiones de TI y seguridad llevada a cabo por Barracuda y Vanson Bourne. Los resultados fueron en gran medida coherentes en todos los países y sectores, por lo que este informe se centra en conclusiones generales y relacionadas con el tamaño.

Los hallazgos muestran que las brechas de seguridad del correo electrónico afectan a la mayoría de las organizaciones. Destacan cómo un panorama de amenazas de correo electrónico cada vez más complejo y desafíos internos como las brechas de habilidades y la falta de respuesta automatizada ante incidentes dificultan que las organizaciones detecten, respondan y se recuperen rápidamente de una brecha.

Los retrasos en los tiempos de respuesta pueden dejar a las organizaciones vulnerables a otros ataques, como el ransomware, y causar daños más generalizados.

Los impactos de una brecha de seguridad del correo electrónico son de gran alcance, desde el tiempo de inactividad hasta el daño reputacional y la pérdida de oportunidades de negocio. Los costes de recuperación afectan especialmente a las pequeñas empresas.

El propósito de este informe es ayudar a las organizaciones a comprender mejor los riesgos e implicaciones de las amenazas de seguridad por correo electrónico y resaltar áreas en las que pueden ser vulnerables.

Metodología

Barracuda encargó a la empresa independiente de estudios de mercado Vanson Bourne la realización de una encuesta global a 2.000 responsables de la toma de decisiones en materia de seguridad que ocupan puestos de TI y negocio en organizaciones de entre 50 y 2.000 empleados de una amplia gama de sectores en Estados Unidos, Reino Unido, Francia, DACH (Alemania, Austria, Suiza), Benelux (Bélgica, Países Bajos y Luxemburgo), los países nórdicos (Dinamarca, Finlandia, Noruega y Suecia), Australia, India y Japón. El trabajo de campo se llevó a cabo en abril y mayo de 2025.

Principales conclusiones

78 %

de las organizaciones experimentaron una brecha de seguridad del correo electrónico en los últimos 12 meses

71 %

de las organizaciones que sufrieron una brecha también fueron víctimas de ransomware durante el año

41 %

sufrieron daños reputacionales, y muchos perdieron nuevas oportunidades de negocio, perjudicando el crecimiento

50 %

detectaron la brecha en menos de una hora

47 %

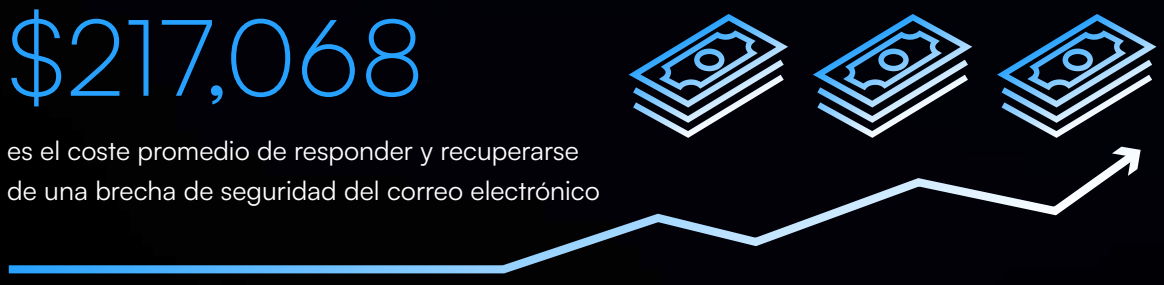
dijeron que las técnicas avanzadas de evasión son el principal obstáculo para una respuesta rápida ante incidentes

44 %

afirman que la falta de respuesta automatizada ante incidentes retrasa la detección, contención y eliminación de amenazas

$217,068

es el coste promedio de responder y recuperarse de una brecha de seguridad del correo electrónico



La mayoría de las empresas experimentan una violación de la seguridad del correo electrónico

La encuesta reveló que el 78% de los encuestados había experimentado una violación de seguridad del correo electrónico en los últimos 12 meses.

Las víctimas fueron atacadas con una amplia gama de tipos de ataque, incluidos phishing y spear phishing (experimentado por el 27% de las víctimas), el fraude del correo electrónico empresarial (experimentado por el 24%) y la usurpación de cuentas (22%).

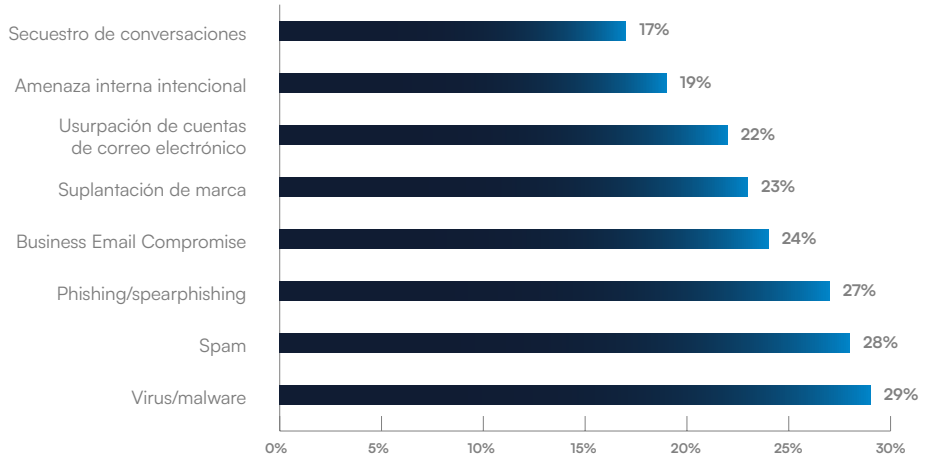


FIGURA 1

¿Qué tipos de ataques basados en correo electrónico han logrado comprometer a su organización en los últimos 12 meses?

El panorama de amenazas de correo electrónico se complica aún más por el hecho de que muchos tipos de ataques por correo electrónico están interrelacionados. Comprender estas relaciones es clave para construir defensas efectivas.

Por ejemplo, el phishing a menudo actúa como el punto inicial de la brecha, abriendo la puerta a amenazas más avanzadas como compromiso del correo electrónico empresarial (BEC), usurpación de cuentas y ransomware. Una vez robadas las credenciales, los atacantes pueden suplantar a usuarios internos para que sus correos electrónicos parezcan más confiables y aumentar la probabilidad nuevos ataques. Las técnicas de spoofing mejoran la efectividad del phishing y BEC al imitar a remitentes de confianza. Mientras tanto, el malware introducido a través del phishing puede automatizar el proceso de ataque, recopilando credenciales adicionales y propagándose por la red.

El BEC es una amenaza dirigida y motivada financieramente. Los atacantes se hacen pasar por personas o entidades de confianza para engañar a los empleados y hacer que transfieran dinero o información sensible. La entrega de malware y ransomware se facilita a través de correos electrónicos de phishing que contienen archivos adjuntos o enlaces maliciosos.

La suplantación de identidad y el spoofing son técnicas utilizadas para engañar a los destinatarios haciéndoles confiar en el remitente. Estas tácticas se emplean comúnmente en el phishing, el compromiso del correo electrónico empresarial (BEC) y campañas de malware. Los atacantes pueden usar el spoofing del nombre mostrado, spoofing de dominio o dominios similares para imitar contactos legítimos, aumentando las posibilidades de que sus mensajes sean abiertos y se actúe en consecuencia.

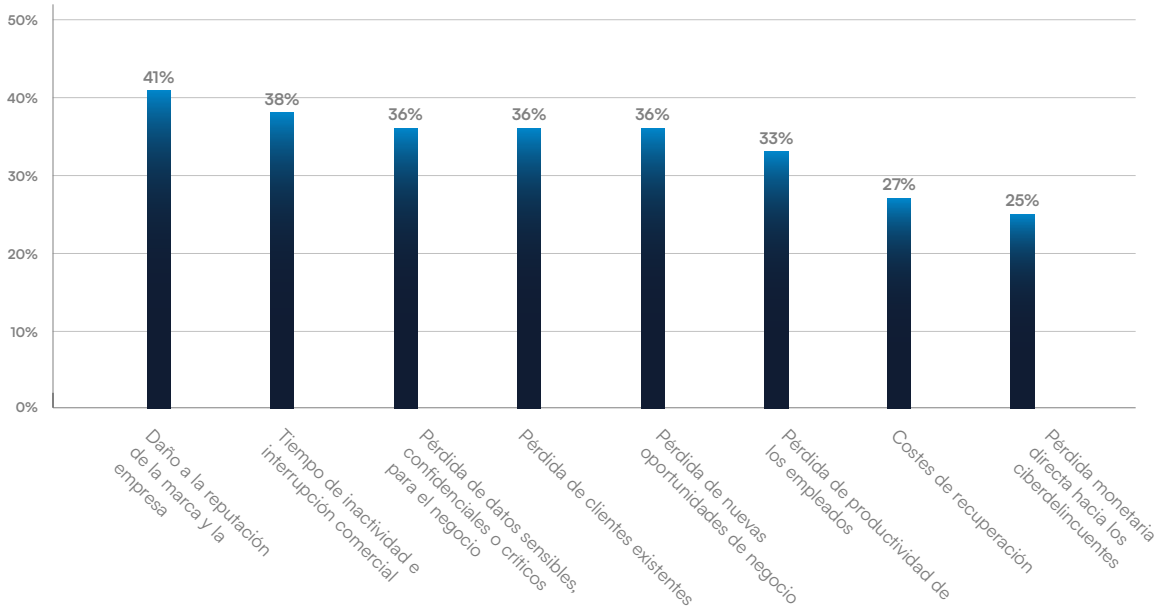
Todos los tipos de amenazas de correo electrónico están creciendo en complejidad, sofisticación y alcance. Muchas de las campañas de phishing más extendidas son desarrolladas y entregadas a gran escala por plataformas bien respaldadas. El daño que estos ataques pueden causar es considerable.

Las brechas de seguridad del correo electrónico frenan el crecimiento empresarial

Según las organizaciones encuestadas, la consecuencia más habitual de una brecha de seguridad del correo electrónico es el daño a la marca y la reputación (mencionado por el 41 % de los participantes). A esto le siguen los impactos operativos, como el tiempo de inactividad y la interrupción de la actividad empresarial (38 %), y la reducción de la productividad de los empleados (36 %). Más de un tercio (36 %) perdió datos confidenciales, y alrededor de una cuarta parte perdió nuevos negocios (27 %) y clientes (25 %).

FIGURA 2

¿Cuál fue el impacto de las brechas de seguridad por correo electrónico en su organización (en general)?



Las consecuencias del daño reputacional pueden extenderse mucho más allá de la percepción pública a corto plazo y tener un impacto profundo y duradero en la salud financiera, la situación legal y la dirección estratégica de una organización.

El impacto en las operaciones comerciales y la productividad, así como las pérdidas financieras, la pérdida de datos (particularmente si esto conduce a incumplimientos normativos y contractuales), el robo de propiedad intelectual y la erosión de la confianza pueden llevar a la pérdida de clientes existentes y nuevas oportunidades de negocio. Esto tiene un impacto tangible en el crecimiento de los ingresos.

Puede ser difícil cuantificar el impacto a largo plazo, pero es posible calcular el coste de responder y mitigar una brecha de seguridad del correo electrónico.

El coste de solucionar una violación de seguridad del correo electrónico afecta más a las pequeñas empresas

Reparar una brecha de seguridad en el correo electrónico cuesta una media de 217.068 $, y las empresas más pequeñas se ven afectadas de forma desproporcionada.

La encuesta abarcó empresas de 50 a 2.000 empleados. El coste medio de mitigación soportado por las empresas de 50 a 100 empleados fue de 145.921 $. Para las empresas de 1.000 a 2.000 empleados, fue de 364.132 $.

Esto significa que el coste medio de recuperación por empleado para las organizaciones más pequeñas (de 50 a 100 empleados) es de 1.946$, frente a un coste medio de solo 243$ para las organizaciones más grandes (de 1,000 a 2,000 empleados).

	50-100 empleados	101-250 empleados	251-500 empleados	501-1,000 empleados	1.001-2.000 empleados
Coste promedio por organización para mitigar la brecha de seguridad del correo electrónico más costosa en los últimos 12 meses	145.921 $	157.804 $	155.804 $	300.751 $	364.132 $
Coste medio por empleado para mitigar la brecha de seguridad del correo electrónico más costosa en los últimos 12 meses	1.946 $	898 $	415 $	400 $	243 $

Las organizaciones más grandes pueden tener mejores defensas y más recursos en términos de habilidades y personal para detectar y responder a incidentes de seguridad. Esto las hace estar mejor preparadas para manejar las violaciones de manera rápida y efectiva, asegurando que cada incidente sea menos costoso en comparación con su tamaño total. Las organizaciones más pequeñas están mucho más expuestas.

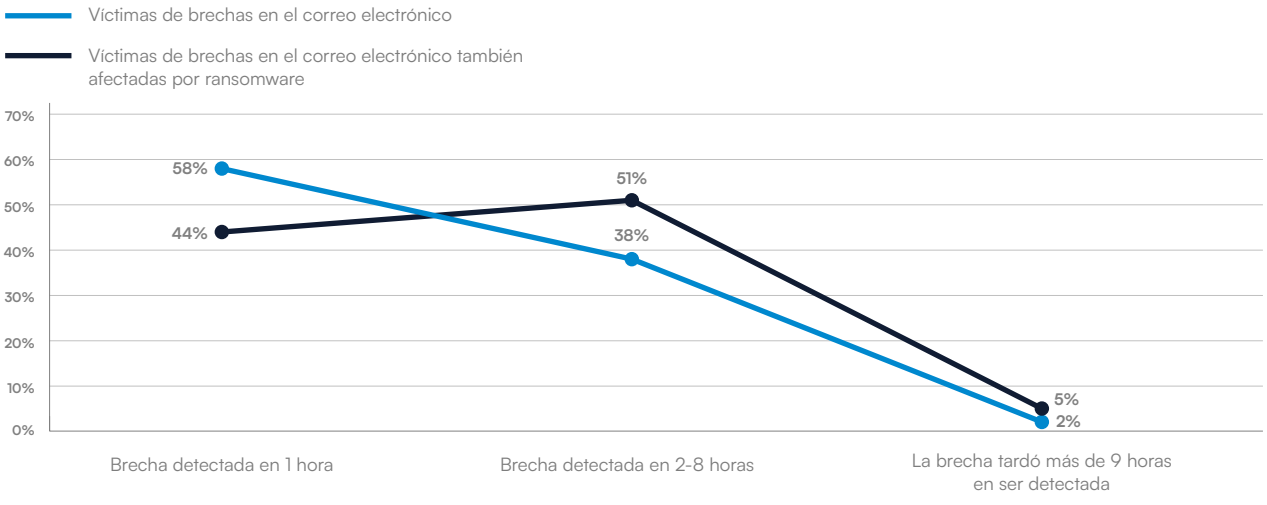
La capacidad de detectar y responder rápidamente a las amenazas de seguridad es fundamental para reducir la exposición al riesgo.

Retrasos en la detección de brechas de correo electrónico y en los tiempos de respuesta aumentan la probabilidad de ransomware.

Existe una correlación entre el tiempo que tarda una organización en detectar y mitigar una brecha de seguridad del correo electrónico y las probabilidades de ser también víctima de un ataque de ransomware exitoso.

FIGURA 3

Tiempo medio para detectar una brecha de seguridad del correo electrónico



La investigación muestra que el 71% de las organizaciones que experimentaron una brecha en la seguridad del correo electrónico informan que también fueron atacadas con ransomware en los últimos 12 meses.

Esto podría deberse a que muchos ataques de ransomware comienzan con un correo electrónico de phishing aparentemente inocuo que ofrece a los atacantes un punto de apoyo —a través de credenciales robadas o un endpoint comprometido— y un canal para entregar ransomware y otras cargas útiles maliciosas a través de archivos adjuntos y enlaces.

Si una brecha de seguridad del correo electrónico no se detecta y contiene rápida y eficazmente, la cadena de ataque tiene tiempo para desarrollarse, permitiendo a los atacantes robar datos, cifrar archivos o establecer acceso persistente a la red.

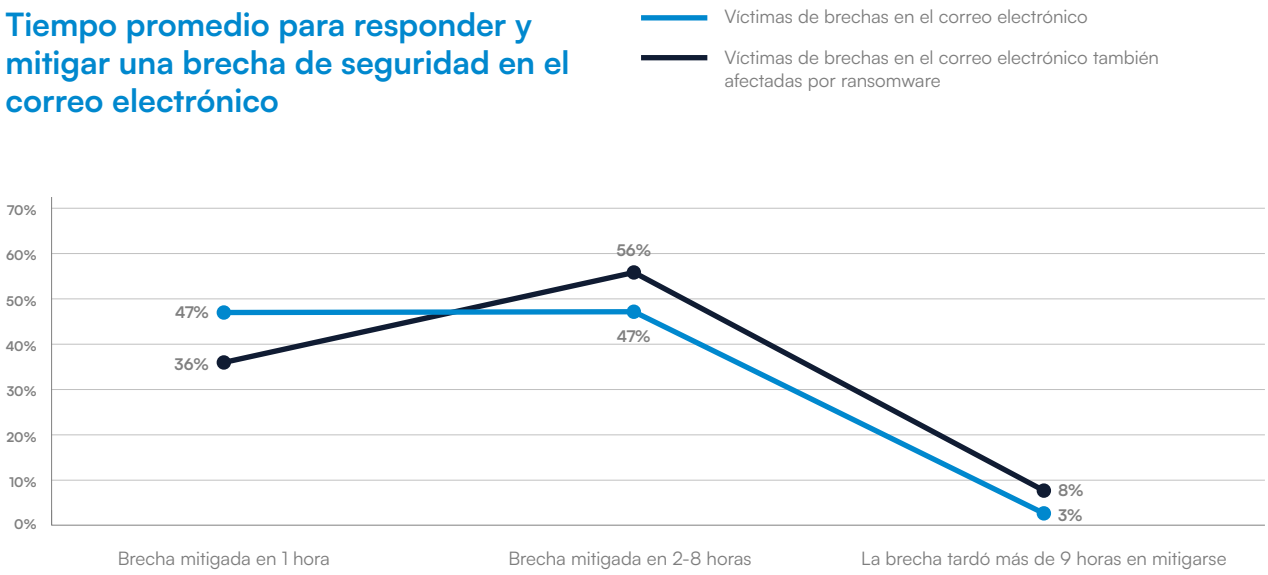
Los hallazgos muestran que las organizaciones que tardaron más en detectar y mitigar una brecha en el correo electrónico tenían una mayor probabilidad de verse afectadas también por ransomware:

- El 58% de las víctimas de brechas de correo electrónico no afectadas por ransomware tardaron menos de una hora en detectar la violación.
- Casi la mitad (47%) de ellos mitigaron la amenaza en menos de una hora tras su detección.

- Sin embargo, en el caso de las víctimas que también sufrieron un incidente de ransomware, la detección y mitigación a menudo llevó más tiempo: el 51% tardó entre dos horas y un día laborable completo en detectar la brecha, y el 56% tardó entre dos y ocho horas después de la detección en mitigar la amenaza.
- En resumen: el 64 % de las víctimas de ransomware tardan más de dos horas en solucionar una brecha de seguridad en el correo electrónico.

FIGURA 4

Tiempo promedio para responder y mitigar una brecha de seguridad en el correo electrónico



Estos hallazgos subrayan la importancia de contar con capacidades efectivas de protección del correo electrónico, respuesta y mitigación en las estrategias más amplias de ciberdefensa.

La respuesta ante brechas se ve obstaculizada por la complejidad de los ataques, los factores humanos y la falta de automatización

Responder rápida y eficazmente a una brecha de seguridad en el correo electrónico no siempre es fácil, y la encuesta destaca los obstáculos que pueden interponerse. Estos se pueden agrupar ampliamente en tres áreas: complejidad del ataque, factores humanos y herramientas de seguridad.

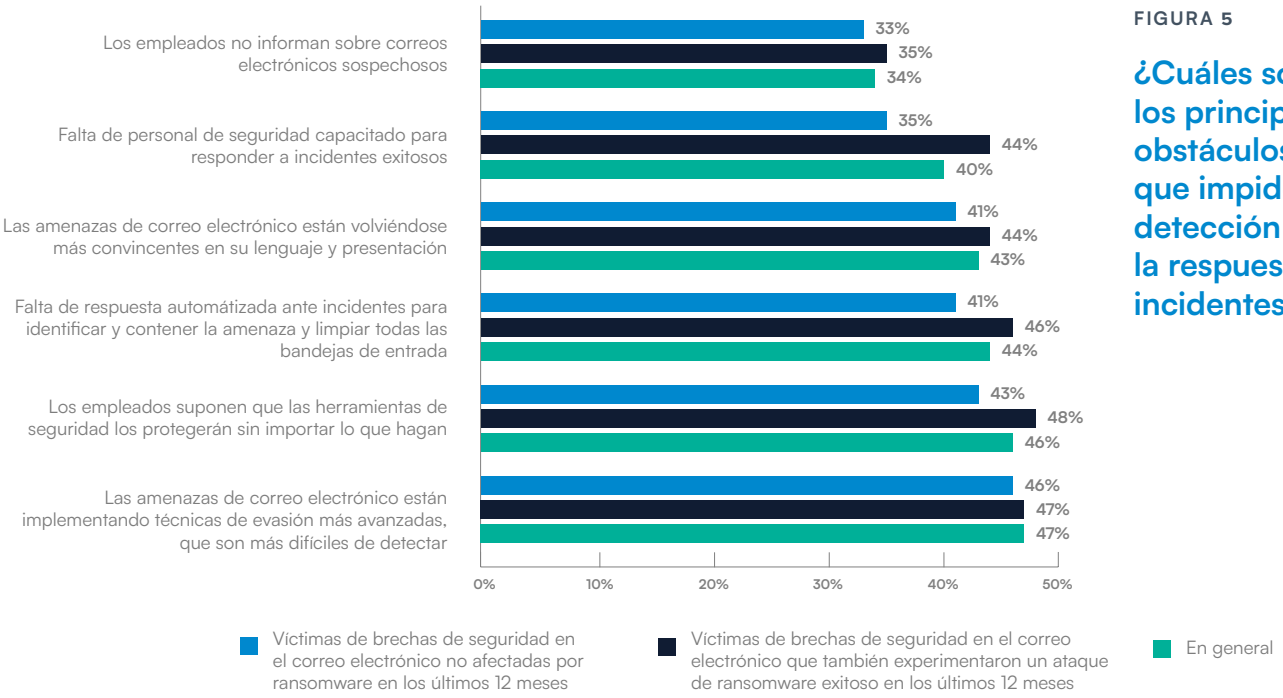


FIGURA 5

¿Cuáles son los principales obstáculos que impiden la detección rápida y la respuesta ante incidentes?

Los obstáculos más citados ofrecen una imagen clara de la complejidad cambiante de las amenazas de correo electrónico y los desafíos internos que afrontan las organizaciones para responder a ellas de manera efectiva una vez que los atacantes han penetrado.

Sofisticación del ataque

- El mayor obstáculo para una respuesta rápida ante incidentes, citado por el 47 % de las víctimas de seguridad del correo electrónico en general, es la naturaleza evolutiva y cada vez más evasiva de las amenazas de correo electrónico, lo que las hace más difíciles de detectar y eliminar de las bandejas de entrada una vez que han logrado acceder con éxito.
- El problema se ve agravado por la creciente sofisticación de los correos electrónicos de phishing. Los atacantes están elaborando mensajes que son lingüísticamente refinados, contextualmente relevantes y visualmente convincentes, a menudo imitando comunicaciones internas o marcas de confianza. Según el 43 % de los encuestados, esto hace más difícil tanto para los usuarios como para las herramientas de seguridad distinguir los correos electrónicos maliciosos de los legítimos.

El factor humano

- Los hallazgos sugieren un nivel de complacencia entre los empleados, ya que el 46 % de los encuestados declaran que sus compañeros asumen que las herramientas de seguridad los protegerán pase lo que pase.
- Alrededor de un tercio (34%) dice que los empleados no informan sobre correos electrónicos sospechosos. Esto también puede permitir que las amenazas persistan en las bandejas de entrada y puede ser un indicio de que los empleados no saben a quién informar sobre los correos electrónicos sospechosos.
- Ambos factores pueden abordarse mediante formación en concienciación en seguridad, incentivos, retroalimentación, mecanismos de reporte sencillos y fomentando una cultura de concienciación proactiva en ciberseguridad.

Herramientas de seguridad

- La falta de capacidades automatizadas de respuesta ante incidentes es una barrera significativa para el 44% de los encuestados. Sin herramientas automatizadas que puedan identificar, aislar y remediar rápidamente las amenazas en las bandejas de entrada de los usuarios, los equipos de seguridad se ven obligados a realizar procesos manuales que son lentos y propensos a errores. Este retraso da a los atacantes más tiempo para explotar la brecha, escalar privilegios o moverse lateralmente dentro de la red.

Escasez de habilidades

- La escasez de personal de seguridad cualificado es un desafío para el 40% de los encuestados.
- Este es el área donde la brecha entre las organizaciones que también fueron víctimas de un ataque de ransomware exitoso y aquellas que no se vieron afectadas es mayor: el 44% de las organizaciones que fueron víctimas de ambos tipos de ataque reportaron esto como una barrera, en comparación con el 35% de las que no se vieron afectadas por ransomware. Si las organizaciones carecen de la experiencia o capacidad para responder eficazmente a una brecha detectada, esto puede llevar a una contención retrasada o una remediación incompleta, permitiendo a los atacantes permanecer en la red y continuar con sus ataques.

Conclusión

La amplia gama de amenazas de correo electrónico que tienen como objetivo a las organizaciones, los impactos tangibles, los costes significativos y la creciente complejidad del panorama de ciberamenazas destacan la importancia de hacer de la protección del correo electrónico una parte integral de las estrategias de defensa cibernética basadas en plataformas.

Un enfoque holístico de la seguridad del correo electrónico debe combinar tecnologías avanzadas de detección impulsadas por IA con la formación de usuarios, respuesta automatizada y una sólida cultura de seguridad.

Las siguientes recomendaciones pueden ayudar

Apoyar a los empleados

1. **Formar regularmente a los** empleados para reconocer el phishing, la ingeniería social y el comportamiento sospechoso del correo electrónico.
2. **Facilite a los empleados el reporte de correos electrónicos sospechosos,** y asegúrese de que los informes se dirijan al equipo adecuado para la investigación y la rápida evaluación.
3. **Limitar el acceso a sistemas y datos sensibles,** según los roles de trabajo. Esto minimiza el impacto del robo de credenciales y el movimiento lateral tras un compromiso de correo electrónico.

Herramientas de seguridad

4. **Implemente la autenticación multifactor (MFA)** para el correo electrónico y otros sistemas críticos. Incluso si las credenciales son robadas a través de phishing, la MFA añade una capa fuerte de defensa contra el acceso no autorizado.
5. **Implemente soluciones de seguridad para el correo electrónico que utilicen IA/ML** para detectar intentos de phishing, malware y suplantación de identidad. Estas herramientas deberían ser capaces de analizar el comportamiento del remitente, el contenido del mensaje y los archivos adjuntos en tiempo real.
6. **Implemente protocolos de autenticación de correo electrónico estándar de la industria** como SPF, DKIM y DMARC para verificar la identidad del remitente y prevenir la suplantación. Estos protocolos ayudan a garantizar que solo los remitentes autorizados puedan usar su dominio.
7. **Automatice la respuesta ante incidentes** utilizando herramientas que puedan identificar y poner en cuarentena automáticamente los correos electrónicos maliciosos después de la entrega, eliminarlos de las bandejas de entrada e iniciar flujos de trabajo de contención. Esto reduce el tiempo de permanencia del atacante y limita la exposición.

Medidas a largo plazo

8. **Aproveche los canales de inteligencia de amenazas** para mantenerse actualizado sobre las amenazas de correo electrónico emergentes, dominios maliciosos y tácticas de los atacantes. Integre estos datos en sus sistemas de detección y plataforma de seguridad más amplios.
9. **Realice auditorías periódicas** de las configuraciones de seguridad del correo electrónico y simule escenarios de ataque (por ejemplo, phishing, BEC) para probar sus capacidades de detección y respuesta.
10. **Comprender y abordar las demandas regulatorias** asegurando que tenga las medidas de seguridad del correo electrónico en su lugar para una detección, respuesta y protección de datos robustas. Esto también ayudará con los requisitos de seguro cibernético.

En el panorama de amenazas dinámico e interconectado de hoy en día, la protección del correo electrónico no se trata solo de detener el Spam o el phishing, sino de prevenir que caiga la primera ficha de dominó en una cadena que podría terminar en una parálisis operativa, pérdida de datos, daño reputacional e impactos comerciales a largo plazo.

Sobre Barracuda

Barracuda es una empresa líder mundial en ciberseguridad que ofrece protección completa frente a amenazas complejas para empresas de todos los tamaños. Nuestra plataforma BarracudaONE, impulsada por IA, protege el correo electrónico, los datos, las aplicaciones y las redes con soluciones innovadoras, XDR gestionado y un panel centralizado para maximizar la protección y reforzar la resiliencia cibernética. Con la confianza de cientos de miles de profesionales de TI y proveedores de servicios gestionados de todo el mundo, Barracuda ofrece defensas potentes que son fáciles de comprar, implementar y usar.

Acerca de Vanson Bourne

Vanson Bourne es un especialista independiente en investigación de mercados para el sector tecnológico. Su reputación en lo referente a análisis sólidos y creíbles basados en la investigación reside en rigurosos principios de investigación y en su capacidad para recabar las opiniones de los principales responsables de la toma de decisiones en todas las funciones técnicas y empresariales, en todos los sectores empresariales y en los principales mercados. Para obtener más información, visita vansonbourne.com.