Anticípese a los ataques avanzados actuales a través del correo electrónico

Servicio gestionado de seguridad del correo electrónico

El correo electrónico es el principal vector de amenazas utilizado en los ciberataques

Todas las empresas sufren el mismo reto: el correo electrónico es al mismo tiempo la herramienta de comunicación profesional más importante y el principal vector de ataque para una violación de la seguridad.

Proteja el correo electrónico de su empresa frente a las amenazas modernas

Los ciberdelincuentes aprovechan el correo electrónico de muchas maneras, ya sea para introducir malware en los sistemas de una organización, robar datos o utilizar ingeniería social con fines lucrativos. Para poder proteger su marca, su reputación y sus datos, su empresa necesita herramientas capaces de detectar y bloquear con rapidez las amenazas avanzadas del correo electrónico entrante.

¿En qué consiste nuestro servicio gestionado de seguridad del correo electrónico?

Nuestro servicio gestionado Advanced Email Security le ayuda a proteger su organización con las competencias y tecnologías de próxima generación más eficaces, y le proporciona la protección más exhaustiva frente a la enorme variedad de amenazas que llegan por este canal.

Resultados demostrados

Cada vez son más las empresas que eligen nuestro servicio gestionado de seguridad del correo electrónico para prevenir:

Ataques de phishing y BEC (vulneración del correo electrónico de empresas)

Los hackers se sirven de la información que recopilan en sitios web de redes sociales para inducir a los usuarios a revelar información confidencial.

Usurpación de cuentas

Los ciberdelincuentes se hacen con el control de una cuenta legítima y la utilizan para realizar acciones maliciosas.

Ataques de día cero y amenazas persistentes avanzadas

Estos ataques utilizan técnicas de hackeo continuas y sofisticadas para conseguir acceso a un sistema y permanecer en él durante un periodo de tiempo prolongado.

INCOPYME
tu tranquilidad tecnológica

¿Sabía que...?

El phishing es un tipo de estafa online en la que el atacante suplanta la identidad de una organización legítima a través de correo electrónico, mensajes de texto o publicidad, con el fin de engañar a la víctima y conseguir que revele información confidencial o bien que instale software malicioso en su dispositivo.

90 %
de los ciberataques que prosperan empiezan por un mensaje de correo electrónico
↘ Más información

4,24 millones de dólares
fue el coste medio global de una violación de datos en 2021
↘ Más información

58 %
de las empresas encuestadas perdió hasta tres horas de productividad como resultado del spam
↘ Más información

Ventajas

- Protéjase frente a los ataques de phishing selectivo y el fraude por correo electrónico.
- Detenga el ransomware y el malware de día cero antes de que lleguen a su buzón de correo.
- Impida con la protección para URL que su equipo haga clic en enlaces maliciosos en cualquier dispositivo.
- Bloquee las amenazas emergentes con inteligencia sobre amenazas en tiempo real.
- Mejore su productividad de forma inmediata controlando el spam.
- Garantice que los mensajes de correo electrónico se entregan siempre y que la productividad no se ve afectada.
- Neutralice el spoofing y los ataques BEC dirigidos contra su empresa.
- Impida los intentos de usurpación de cuentas y supervise los buzones de correo interno para detectar cualquier indicio de compromiso.

Pasos siguientes

Para obtener más información sobre nuestro servicio gestionado de seguridad del correo electrónico, póngase en contacto con nosotros:

Richard Romero
richard@incopyme.com 0034645715079

Evite la pérdida de productividad debida al spam

El spam no es solo molesto: también afecta a la productividad de la empresa y a la capacidad de los empleados para concentrarse en su trabajo. El tiempo que dedican a borrar los mensajes innecesarios que abarrotan su buzón de correo es solo la mitad del problema. Además, el spam puede causar graves perjuicios infectando los ordenadores de los empleados con software malicioso capaz de dañar los sistemas y robar información personal o empresarial.

Proteja los buzones de Microsoft 365, Google Workspace u otro tipo de correo basado en la nube o local frente a las amenazas avanzadas

Usurpación de cuentas

La usurpación de cuentas de Microsoft 365, Google Workspace u Open-Xchange mediante el phishing de credenciales es una de las tres principales amenazas más frecuentes del correo electrónico. Nuestros servicios no solo le protegen frente al phishing que intenta captar las credenciales de sus empleados, sino que también supervisan sus cuentas de correo electrónico para detectar conductas sospechosas que indiquen una posible violación de la seguridad y mitigar rápidamente cualquier brecha en sus buzones.

BEC

En los ataques BEC, el agresor utiliza la suplantación de identidad (por ejemplo, haciéndose pasar por un ejecutivo o un consejero) para engañar al usuario y conseguir que realice una transferencia bancaria fraudulenta o facilite información confidencial o sensible. Su empresa necesita una seguridad del correo electrónico complementaria que detecte y detenga los ataques avanzados —que no llevan carga maliciosa— antes de que lleguen a los usuarios. También es importante mitigar rápidamente el impacto de las violaciones de seguridad —si llegan a producirse—, sin interrumpir la entrega normal de mensajes.

Microsoft 365 · Google Workspace · Exchange · OX

Y muchas otras...

Proteja el correo electrónico de su empresa frente a cualquier ataque.