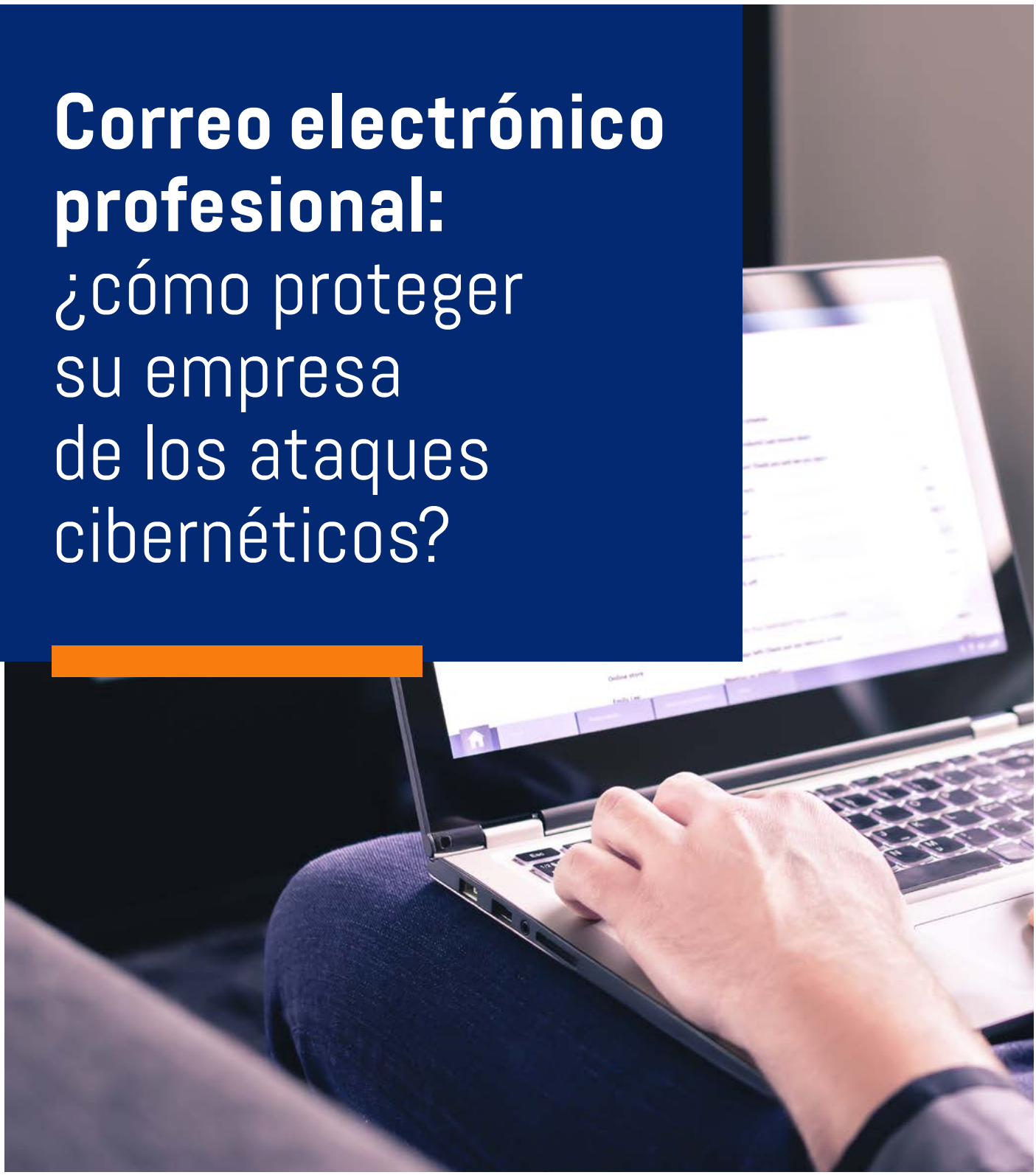
Alinto

Libro blanco

Noviembre de 2021

Correo electrónico profesional: ¿cómo proteger su empresa de los ataques cibernéticos?



Contenido

Apretar las mallas de la red

Sólo una de cada dos empresas afirma estar equipada y preparada para hacer frente a un ciberataque1 . Este es un triste hecho que lleva a las organizaciones a replantearse la seguridad de su red informática, y más concretamente de su correo electrónico empresarial.

De hecho, la mayoría de los ataques informáticos provienen de correos electrónicos fraudulentos. Y las técnicas y tecnologías utilizadas por los hackers son cada vez más sofisticadas. Ahora se dirigen a todas las empresas: desde las más pequeñas hasta las multinacionales, aprovechando la escasa concienciación de los empleados respecto a los correos electrónicos maliciosos.

Las empresas más vigilantes aplican estrictas medidas de seguridad: cortafuegos, parches, antispam, etc. Sin embargo, estas protecciones, a menudo vinculadas a las soluciones de red, sistema y mensajería implantadas, tienen sus límites. Un correo electrónico puede colarse en la red.

En este libro blanco, echamos un vistazo a la situación actual de los ciberataques, revisamos las mejores prácticas para reforzar la seguridad de su correo electrónico y ofrecemos consejos sobre cómo proteger mejor su organización.

[1] 6to edición del barómetro anual de CESIN

Seguridad del correo electrónico : estado de la cuestión

Nunca se repetirá lo suficiente, el correo electrónico es el canal preferido para ciberataques. Y cada año es peor, a pesar de la mejora en la seguridad de la mensajería personal y profesional, la conciencia y la difusión de alertas sobre phishing y ciberataques. Desde Por otra parte, los ciberdelincuentes utilizan cada vez más programas maliciosos sofisticados y sus técnicas son más avanzadas, por lo que pueden utilizarse para confusión.

El ransomware, el phishing, el malware... son amenazas para empresas, que deben por tanto extremar la vigilancia y concienciar a sus empleados sobre colaboradores. Sobre todo porque los ciberdelincuentes navegan por la pandemia del Coronavirus, utilizando el miedo para fomentar el clic.

Para aclarar la situación, le ofrecemos un resumen de la misma.

Ciberseguridad:
el preocupante aumento de los ataques por correo electrónico

En 2020, los ciberataques se habrán cuadruplicado respecto a los años anteriores[1]. Los ciberdelincuentes están ahora mejor organizados, envían numerosos correos electrónicos fraudulentos y apuntan a las vulnerabilidades de las redes informáticas de las empresas. Los ataques son industrializados, planificados. Estamos lejos de una persona que actúa sola detrás de su ordenador.

He aquí algunas cifras que ilustran la situación actual y la vulnerabilidad relacionada con la mensajería en Francia:

- El ransomware representa El 11% del volumen total de correos electrónicos maliciosos[2] .
- El 80% de las empresas francesas ciberatacadas en 2020 fueron atacadas a través de correos electrónicos de phishing o spear-phishing[3] .
- En 2020, una de cada cinco empresas declara haber sufrido al menos un ataque de ransomware durante el año[4].
- Sólo una de cada dos empresas confía en su capacidad para hacer frente a un ciberataque[5] .

- La crisis sanitaria conlleva nuevos riesgos: aumento del 35% de los ciberataques[6] .

- El 57% de las empresas tiene previsto aumentar su presupuesto de ciberseguridad[7] .

- El 85% de las empresas quiere adquirir nuevas soluciones técnicas para mejorar su seguridad informática[8].

- El 75% de los correos electrónicos recibidos son indeseados[9].

- Las denuncias de ciberataques a la Administración por parte de los profesionales han aumentado un 30% respecto a 2019[10] .

El desarrollo del teletrabajo, el miedo inducido por la pandemia, el desarrollo de la nube, la profesionalización de los ataques por correo electrónico explican esta evolución. No hay indicios de un cambio de tendencia: es probable que el fenómeno continúe durante los próximos años y siga siendo una verdadera preocupación para las organizaciones.

Ciberataques: importantes consecuencias para las empresas

Es difícil calcular el coste de un ciberataque. Esto no sólo se refleja en las consecuencias económicas, sino también en el impacto en la reputación de la empresa, el debilitamiento de la infraestructura informática o las dificultades operativas para las distintas líneas de negocio.

En 2020, el 58% de los ciberataques tuvieron un impacto probado en el negocio, con una interrupción directa de la producción en el 27% de los casos[11].

Las principales consecuencias de los atentados[12] pueden desglosarse como sigue:

- Robo de datos (30%)
- Denegación de servicio (29%)
- Bloqueo de la actividad tras la codificación
- de datos por ransomware (24%)
- Robo de identidad (23%)

Un estudio de Bessé muestra que el riesgo de fracaso de una empresa aumenta un 50% en los tres meses siguientes al anuncio de un ciberataque. Este riesgo alcanza a veces incluso el 80%[13].

Otro estudio realizado por el Instituto Ponemon de IBM reveló que el 80% de las empresas francesas no tienen un plan de respuesta a incidentes. Otro dato significativo es que una empresa tarda una media de 201 días en descubrir que ha sido víctima de un ciberataque. Las consecuencias directas también pueden afectar a los clientes si sus datos personales han sido robados.

Así, un simple clic en un enlace de un correo electrónico puede debilitar irremediablemente a toda la empresa. Por eso es importante seguir concienciando a los empleados, pero también reforzar la seguridad informática mediante diversas soluciones de protección del correo electrónico.
rendimiento.

---

[1] Los ciberataques se cuadruplicaron el año pasado,
según un experto en ciberseguridad - France TV info
[2] Intervención Devensys - Métodos para mejorar la seguridad de su correo electrónico 2018
[3] Los ciberataques más comunes contra las empresas francesas - Statista
[4 a 8] 6to edición del barómetro anual de CESIN
[9] Mensajería: cifras y amenazas - dsisionnel de seguridad
[10] Ciberseguridad: más informes en 2020 - revista vie-publique
[11] 6to edición del barómetro anual CESIN
[12] Los ciberataques más comunes contra las empresas, CESIN y OpinionWay
[13] En un panel de pymes

Algunos ejemplos de ciberataques y sus consecuencias :

- Un hospital de Nueva Jersey (EEUU) pagó un rescate de más de 600.000 dólares (2020).

- A Verne Harnish, director general de Gazelles Inc. le robaron 400.000 dólares de su cuenta bancaria cuando unos hackers accedieron a su ordenador e interceptaron los correos electrónicos entre él y su asistente (2019).

- EasyJet ha anunciado que ha sido víctima de un importante ciberataque: más de 9 millones de datos de clientes (direcciones de correo electrónico e información de viaje), incluyendo Se accedió ilegalmente a los datos de 2.000 tarjetas bancarias (2020).

- La Universidad de California en San Francisco (UCSF) sufrió un ataque de ransomware que paralizó el acceso a los datos de su red informática. Al final, la Universidad aceptó pagar un rescate de aproximadamente un millón de euros (2020).

Cuatro buenas prácticas para prevenir los ciberataques relacionados con el correo

El punto de entrada preferido por los hackers en Internet es el correo electrónico. Y el crecimiento masivo del teletrabajo provocado por la pandemia ha acentuado la número de ataques, especialmente de ransomware. De hecho, el Club de Expertos de la Información y la Seguridad Digital (Cesin) estima que para 2020, el 57 de empresas han sido víctimas de un ataque informático. Una cifra se cuadruplicó en un año. Sin embargo, ¡no tiene por qué ser así! Existen soluciones para proteger su empresa. Esto requiere la adopción de varias buenas prácticas, que entregamos en este artículo.

Buena práctica nº 1
Sensibilización de los empleados

Lo primero que hay que hacer es comunicar a sus equipos los riesgos de los ciberataques y las consecuencias que pueden tener para la empresa. Esto significa explicar cómo reconocer un correo electrónico sospechoso y las diversas precauciones que hay que tomar para asegurar el acceso a su correo electrónico. Se animará a sus empleados a establecer una contraseña segura, limitar el envío y la apertura de archivos adjuntos, no hacer clic en enlaces que parezcan sospechosos, no divulgar información confidencial, comprobar la identidad del remitente, etc.

También es importante destacar la importancia de notificar al departamento de TI en caso de sospecha de correo electrónico fraudulento. La reacción debe ser rápida para poder iniciar el procedimiento adecuado, antes de que el virus se extienda y cause daños importantes.

Buena práctica #2
Proteger los datos sensibles

Desde la entrada en vigor del RGPD, las cuestiones de ciberseguridad son aún más estratégicas para las empresas. La seguridad del acceso a la SI y a la información personal debe estar garantizada.

Para asegurar los datos, es esencial aplicar una política rigurosa de gestión de contraseñas. Esta es la primera palanca para asegurar los puestos de trabajo de sus empleados. Las contraseñas deben ser complejas, difíciles de adivinar, confidenciales y renovadas regularmente.

Para mayor seguridad, configure los puestos de trabajo de sus empleados para que se bloqueen automáticamente tras unos minutos de inactividad. También es esencial proteger los archivos que contienen datos sensibles y restringir el acceso a las personas autorizadas.

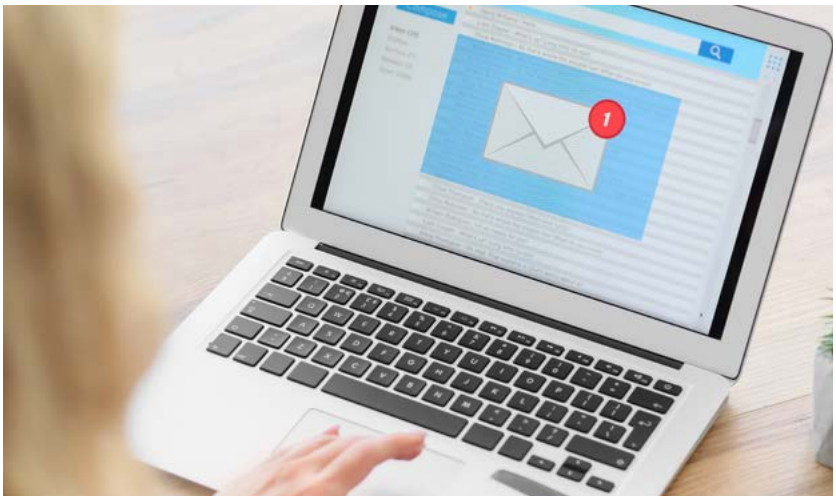
Siempre con el objetivo de asegurar la SI, es importante encriptar los datos sensibles, como los relativos a la salud, la información de pago, etc. Todas estas precauciones son inseparables de la protección de la infraestructura de la red con la instalación de cortafuegos, routers de filtrado, sondas anti-intrusión, sistemas de equilibrio de carga y detección de ataques DDoS, etc.

Buena práctica #3
Mantener el control del tráfico de correo

El correo electrónico sigue siendo el canal de comunicación más utilizado en el mundo. Los usuarios reciben cientos de correos electrónicos al día. Esto es estresante e ineficiente, pero también tiene un impacto significativo en la exposición a los ciberataques. Como muestra nuestro informe de seguridad del correo electrónico, más del 75% de los correos electrónicos son no deseados.

Por ello, el control del tráfico de correo electrónico es esencial: es necesario garantizar que los correos electrónicos fraudulentos se queden a las puertas del SI de la empresa. Pero este filtrado debe ser fino y preciso para no eliminar correos electrónicos válidos y útiles para los empleados.

Por eso es importante establecer y adaptar constantemente las reglas de filtrado, hacer evolucionar las listas blancas y negras, colocar en zona de cuarentena los correos electrónicos no fraudulentos pero sospechosos de ser comerciales. Los usuarios podrán acceder a ella para no perderse ninguna información importante.



Buena práctica #4
Despliegue de una solución de asegurar el correo electrónico

Para reforzar la seguridad del correo electrónico de su empresa, es esencial desplegar un software de protección del correo electrónico (como antispam o antivirus). Estas soluciones se actualizan a medida que aparecen nuevos ciberataques. Se adaptan perfectamente a las diferentes soluciones de correo electrónico profesional, empezando por Microsoft 365 Exchange. Estas herramientas filtran el spam mediante la comprobación de múltiples criterios, hacen una lista negra automática de determinados remitentes, protegen su reputación (por el envío de correos masivos, etc.).

Los proveedores de soluciones de mensajería ofrecen soluciones antispam nativas, pero no siempre (o rara vez) son suficientes. Por lo tanto, es esencial asegurar una protección reforzada gracias a herramientas dedicadas, como Alinto Protect. Las ventajas son numerosas: protección del correo electrónico, bandeja de entrada más limpia, filtrado más fino, gestión de la cuarentena, ahorro de tiempo en la gestión del correo electrónico...

Para recordarles estas cuatro recomendaciones esenciales, no dude en anotar todas las buenas prácticas en un documento a disposición de sus empleados. La comunicación y la concienciación del equipo también son esenciales para la correcta protección del correo electrónico de su empresa.

¿Por qué las soluciones de correo electrónico tienen antispam incorporado? no son suficientes?

Muchas empresas utilizan el software antispam que se ofrece con sus soluciones de correo electrónico. No ven el sentido de optar por una solución adicional. Algunos ni siquiera utilizan uno. Sin embargo, esto es un verdadero reto para las organizaciones. De hecho, el correo electrónico es el principal punto de entrada de los ciberataques.

Además de concienciar a los empleados sobre las mejores prácticas para reconocer los correos electrónicos fraudulentos, es importante reforzar la seguridad de su sistema de correo electrónico profesional. Porque muy a menudo, el software antispam ofrecido por su proveedor no es suficiente. Le explicamos por qué.

El antispam integrado no es lo suficientemente eficaz

El software antispam integrado en los sistemas de correo electrónico filtra el correo no deseado mediante reglas de filtrado generales y predefinidas. Estas reglas son difíciles de administrar y no son fácilmente adaptables a las necesidades de los usuarios y a la aparición repentina de nuevas amenazas. Por lo tanto, se trata de una protección incompleta del sistema de correo electrónico, que bloquea los correos electrónicos de las listas de spam, que tienen objetos o archivos adjuntos dudosos.

La prueba: en 2016, AV Comparatives envió 127.800 mensajes de spam a cuentas que tenían proveedores de servicios de correo electrónico. Los índices de detección fueron muy bajos: el 89,87% del spam llegó a uno de los proveedores. Esto demuestra que es importante ir más allá de las versiones básicas - aparentemente gratuitas, al menos sin coste adicional - y conseguir una solución complementaria más potente.

El más potentes son muy caros

Por supuesto, los proveedores de correo electrónico ofrecen versiones mejoradas y de pago de su software antispam (como Microsoft Advanced Threat Protection / Microsoft 365 Defender). Estos ofrecen funciones más avanzadas. Por ejemplo, pueden ser configurados por los administradores (visualización, modificación, configuración). También es posible crear reglas personalizadas para cada usuario, que siempre tendrán prioridad sobre las reglas globales.

Estas versiones también ofrecen procesos automatizados mediante inteligencia artificial. Van más allá e identifican las campañas comerciales que escapan al filtrado de primer nivel. También se dispone de cuadros de mando para analizar la evolución del tráfico de correo y el número de spam, correo basura, etc.

Sin embargo, estas soluciones son bastante caras y se facturan en función del número de usuarios. Por término medio, debería contar con varias decenas de euros al mes y por usuario. Haga el cálculo en función de su número de empleados: es una cantidad considerable para las empresas, que a veces prefieren no utilizarlas. De este modo, dejan el campo más abierto a los ciberdelincuentes.

Antispam: ¿qué soporte ofrece su proveedor de correo electrónico?

Los proveedores de mensajería empresarial más populares son a veces víctimas de su propio éxito. El inconveniente es que su soporte no es fácilmente localizable o disponible. En caso de incidente, es importante tener acceso a un apoyo eficiente y receptivo. Además, a menudo es necesario recurrir a integradores para desplegar estas soluciones, lo que limita la relación directa con el editor.

Al recurrir a un editor de soluciones antispam de tamaño humano como Alinto, pone todas las posibilidades de su lado para beneficiarse de un socio reactivo, accesible y atento a sus problemas. Esta es una ventaja importante cuando se conocen las consecuencias de una indisponibilidad del correo electrónico o de un ciberataque. Asegúrese de obtener la información correcta antes de hacer su elección, ya que no todos los proveedores de servicios ofrecen el mismo nivel de apoyo.

Aunque los principales proveedores de correo electrónico ofrezcan un sistema antispam de serie, es esencial reforzar la seguridad de los buzones de sus empleados. Hay una amplia gama de soluciones complementarias a su disposición. Para hacer una buena elección, define una lista de criterios que consideres esenciales: soporte, funcionalidad, ergonomía, proximidad, bases de precios, etc. No lo olvides: es el software el que se adapta a tus retos y no al revés.

Cinco características clave para su software de seguridad correos electrónicos

Está convencido: necesita protección adicional contra su correo electrónico profesional. Sin embargo, es difícil elegir en el de soluciones disponibles. Entre las soluciones antispam integradas directamente en el Si está buscando un servicio de correo electrónico o un software adicional, su corazón está en el lugar correcto.

En nuestra opinión, hay cinco características esenciales. Deberían debe ser ofrecida por su futuro proveedor. Descúbralos en este artículo.

Característica nº 1

Filtrar los correos electrónicos entrantes

Por supuesto, su futuro software de seguridad de correo electrónico debe ofrecerle un filtrado eficaz de los correos electrónicos entrantes. Esto puede hacerse de varias maneras:

- Filtrado de correo electrónico basado en la reputación: filtrado de spammers conocidos, consulta de bases de datos internacionales de reputación...
- Lista blanca: selección de remitentes cuyos correos electrónicos la empresa acepta.
- Lista negra: lista de remitentes cuyos correos electrónicos la empresa rechaza.
- Análisis de contenido: bloqueo de un mensaje según su contenido (análisis de palabras, enlaces, imágenes, archivos adjuntos, etc.).

Para una mayor agilidad y adaptabilidad, elija una solución que le permita modificar, adaptar, eliminar o añadir filtros fácilmente, en unos pocos clics y según las necesidades de sus usuarios finales.

Característica nº 2
Antispam y antivirus

En relación con la primera funcionalidad, es importante, por supuesto, elegir una solución de protección con un potente antispam y antivirus. En efecto, mientras que la primera característica permite asegurarse de la legitimidad del remitente, la segunda puede enviar spam o un virus sin saberlo. Por lo tanto, el mensaje debe ser analizado en profundidad. Muchos correos electrónicos no deseados consiguen sortear las herramientas antispam integradas en las soluciones de correo electrónico y acaban en las bandejas de entrada de sus usuarios.

Opte por una solución basada en tecnologías potentes, que interroga a las bases de datos internacionales compartidas, aprovecha también sus propias bases de datos de spam que se adaptan a la semántica local y somete los correos electrónicos a diferentes programas antivirus para un mejor filtrado de las ciberamenazas.

Más concretamente, para que el software defina con rigor si el correo electrónico recibido es spam, analiza varios elementos del mismo: enlaces, asunto, archivos adjuntos, imágenes, etc. según unos criterio

Característica #3
Proteger su reputación

Es importante que su nombre de dominio tenga una buena reputación para que los correos electrónicos enviados por sus usuarios, especialmente los comerciales, no sean considerados como spam. Para ello, se establece una puntuación del remitente. Tiene en cuenta varios elementos, como la tasa de rebote duro o blando, las tasas de apertura, las quejas por spam, la limpieza periódica de sus bases de datos, el uso de protocolos de identificación y la calidad de sus correos electrónicos (evite los archivos adjuntos, las imágenes o los objetos demasiado publicitarios).

El propósito de la puntuación del remitente es evitar ser incluido en la lista negra y aumentar la capacidad de entrega de los correos electrónicos de sus empleados.

Característica #4
El BCP (Plan de Continuidad de Negocio)

La imposibilidad de acceder a la bandeja de entrada del correo electrónico puede tener consecuencias desastrosas para la empresa. Sin embargo, esto es lo que puede ocurrir en caso de fallo del sistema o de indisponibilidad de una infraestructura informática.

Por eso le aconsejamos que opte por una solución de correo electrónico con un Plan de Continuidad de Negocio (o BCP). De este modo, sus usuarios podrán seguir utilizando sus buzones a través de un sistema de webmail de reserva, con total transparencia, y no se verán afectados por la indisponibilidad del servidor de correo, aunque esté en la nube de un actor principal. Ninguno de ellos puede garantizar u ofrecer una disponibilidad del 100%.

Además, en cuanto se restablece el acceso al servidor, los intercambios de correo electrónico realizados durante la interrupción se vuelven a sincronizar con el sistema de mensajería para que no se pierda ninguna información. Una verdadera ve

Característica #5
Integración con el entorno existente

Más allá de las funcionalidades, la facilidad de implantación puede marcar la diferencia. Opte por una solución de protección que se adapte a su entorno de trabajo: proveedor de correo electrónico, alojamiento, necesidades de personalización de las reglas en función de los usuarios, autonomía de uso de la solución, disponibilidad de APIs, etc.

Esto es esencial para reforzar la protección de su mensajería y mantener su autonomía de gestión. Ya sea en las instalaciones o en la nube, en las instalaciones o subcontratada, su futura solución debe adaptarse a sus necesidades, y no al revés.

Por supuesto, esta lista de características «imprescindibles» no es exhaustiva. Sin embargo, en nuestra opinión, estos son los criterios esenciales a tener en cuenta a la hora de elegir una solución de protección para el correo electrónico de su empresa. Si quiere saber más sobre esto, póngase en contacto con nosotros.

¿Qué apoyo se necesita para desplegar un ¿refuerzo antispam?

Como hemos visto anteriormente, la funcionalidad de su software de seguridad de correo electrónico es fundamental. Pero hay otro criterio, no menos importante, que debe tenerse en cuenta: el apoyo. Ya sea durante la definición de su proyecto, durante el despliegue de la solución o en caso de que surjan nuevas preguntas a posteriori, opte por un proveedor de servicios local que actúe como un verdadero socio.

¡Y eso es lo que ofrecemos en Alinto! Descubra en este artículo cómo garantizamos el apoyo a nuestros clientes en el centro de nuestra solución.

Software antispam : experiencia y apoyo sobre todo

No hace falta repetirlo, la protección de su correo electrónico profesional es estratégica para su empresa. Por eso es importante recurrir a un socio que lo lleve en su ADN y que tenga un conocimiento real de la seguridad del correo electrónico. Y ese es el punto fuerte de Alinto.

Desde hace más de 20 años, los expertos de Alinto acompañan a las empresas en la gestión de sus sistemas de mensajería profesional. Respondemos a sus expectativas, seguimos las evoluciones y tendencias en materia de ciberataques y proponemos funcionalidades cada vez más avanzadas. Dedicamos El 30% de nuestra facturación se dedica a la investigación y el desarrollo para ofrecer soluciones cada vez más eficaces para proteger los sistemas de correo electrónico de nuestros clientes. Gracias a varias adquisiciones de empresas especializadas en la seguridad del correo electrónico, disponemos de todas las competencias y conocimientos necesarios para garantizar la protección de sus buzones de correo electrónico, y más allá de sus sistemas de información.

El servicio de asistencia es la piedra angular de nuestra empresa. Gracias a un sistema de tickets, nuestros expertos son alertados en tiempo real de las situaciones que encuentran sus clientes. Así, pueden dar una respuesta o tomar decisiones adaptadas al problema en un plazo proporcional a los riesgos.

Despliegue de soluciones antispam: la capacidad de respuesta es la palabra clave

En relación con el servicio de asistencia al cliente, los equipos de consultores de Alinto están a su disposición durante todas las etapas de su proyecto. En la fase previa, ayudándole a enmarcar su proyecto. Durante el despliegue, acompañándole a instalar el software, y a parametrizar las funcionalidades necesarias. Y después, con la respuesta a sus preguntas, el mantenimiento, el apoyo...

La escala humana y la estabilidad de nuestros equipos nos permiten conocer bien a nuestros clientes y sus retos. Somos capaces de responder rápidamente a las distintas necesidades y de comunicarnos eficazmente entre nuestros distintos departamentos para ofrecer una solución adecuada y rápida. Nuestro software, y por tanto su protección, se beneficia de esta agilidad. Sabemos lo problemática que puede ser la interrupción de su servicio de correo electrónico, por lo que la proactividad es la palabra clave de nuestros servicios.

Más allá del antispam : optimización de la gestión del sistema de mensajería

Para proteger el correo electrónico de su empresa, no basta con instalar un software antispam, aunque sea imprescindible. Es importante mirar más allá para optimizar la gestión y la protección de sus correos electrónicos. Así que opte por un software que ofrezca funciones adicionales.

En Alinto ofrecemos, además de la protección antispam y antivirus:

- Una solución de archivo, útil para cumplir con la requisitos reglamentarios. Tú eliges lo que quieres conservar y lo que no, puedes cambiar el reglas, frecuencia... y son alertados antes de que los correos sean destruidos.

- Un relé de correo SMTP para asegurarse de que envía correos electrónicos «limpios» y no pone en peligro la reputación de su dominio de correo electrónico.

- Encriptación, que asegura los correos electrónicos salientes con un sistema de encriptación, necesario en los intercambios de ciertas industrias. Sólo los directores impactado por la encriptación, que sigue siendo totalmente transparente para los usuarios. Servicios de fax y SMS en la nube para ofrecer una solución única para todos sus canales de comunicación. Gracias a las API o directamente a través de los correos electrónicos, benefíciese de toda la experiencia de Alinto para desmaterializar sus faxes y SMS.

Alinto también ofrece otros servicios relacionados con el correo electrónico. Con una constante: la proximidad. ¿Tiene un proyecto o preguntas? No dude en ponerse en contacto con nosotros.

Conclusión

Con la amenaza de los ciberataques cada vez más insidiosa, la protección del correo electrónico empresarial ya no es una opción para las organizaciones. Y ya no basta con conformarse con las versiones estándar del software antispam.

Por eso, optar por un software de protección del correo electrónico empresarial es la mejor opción para poner todas las posibilidades de su lado. También es importante concienciar a los empleados, comunicar sobre las buenas prácticas cotidianas y vigilar y anticipar las tendencias de ciberseguridad.

Sobre nosotros

Fundada en 2000, Alinto es una empresa especializada en el negocio del correo electrónico: servicio de correo electrónico en modo SaaS, antispam, servidor de correo electrónico... a través de varios productos:

- **Alinto Protect:** el relé de correo electrónico seguro que inmuniza contra los riesgos de Internet garantizando el acceso permanente a los correos electrónicos.

- **Alinto Gateway:** El relé de correo SMTP permite que los servidores o aplicaciones envíen correos electrónicos para garantizar un tráfico denominado «limpio».

Presente en Francia, Suiza y España, Alinto cuenta con más de 30 empleados y proporciona un servicio de calidad a más de tres millones de usuarios. Cada día se envían más de 15 millones de correos electrónicos gracias a sus servicios de correo electrónico.

El grupo Alinto aglutina varias entidades desde 2016 para posicionarse como un actor principal en la mensajería electrónica. Está compuesta por las siguientes empresas:

- Cleanmail: empresa suiza especializada en el filtrado antispam en la nube desde 2002
- SerenaMail: especialista español en seguridad del correo electrónico (filtrado de spam).
- Alinto: servicios de mensajería segura.

Esto permite al grupo consolidar su posición en el mercado y ampliar su desarrollo internacional.

Lyon (sede)
15 quai Tilsitt
69002 Lyon
+33 481 09 01 10

Barcelone
Avda. Diagonal, 434
08037 Barcelona
+34 91 005 29 64

Zurich
Gertrudstrasse 1
CH-8400 Winterthur
+41 52 208 99 66

Alinto

www.alinto.com