HORNETSECURITY

CYBERSECURITY REPORT 2025

Un Análisis Exhaustivo del Panorama de Amenazas de Microsoft 365 Basado en el Estudio de

55.6 Mil Millones de Correos Electrónicos

hornetsecurity.com

HORNETSECURITY
CSR2025

SOBRE HORNETSECURITY

Hornetsecurity ayuda a las empresas y organizaciones de todos los tamaños a centrarse en lo que realmente importa: su actividad. Lo hace protegiendo las cargas de trabajo de Microsoft 365, asegurando las comunicaciones por correo electrónico, protegiendo los datos y garantizando la continuidad del negocio y el cumplimiento normativo. Todo esto, gracias a soluciones en la nube de última generación.

Nuestro producto estrella, 365 Total Protection, es la solución más completa del mercado para la seguridad en la nube de Microsoft 365. Ofrece protección para el correo electrónico, herramientas para cumplir con normativas, gobernanza y copias de seguridad.

¿QUÉ ES EL CYBERSECURITY REPORT 2025?

El Cybersecurity Report 2025 de Hornetsecurity es un análisis anual sobre las amenazas que acechan a Microsoft 365. Este informe se basa en datos reales recopilados y estudiados por el equipo experto del Security Lab de Hornetsecurity. Nuestras soluciones de ciberseguridad procesan más de 4.500 millones de correos electrónicos al mes. Analizando estas amenazas, junto con un conocimiento detallado del panorama global de la ciberseguridad, el Laboratorio identifica las principales tendencias, desvela las tácticas de los ciberdelincuentes y elabora proyecciones sobre posibles amenazas futuras. Gracias a este informe, las empresas pueden adelantarse y tomar medidas preventivas.

¿QUÉ ES EL SECURITY LAB?

El Security Lab es una división especializada de Hornetsecurity que analiza las amenazas de seguridad más críticas, con un enfoque particular en el ecosistema de Microsoft 365 y la protección del correo electrónico. Contamos con un equipo internacional de expertos en ciberseguridad, ingeniería de software y ciencia de datos, con amplia experiencia en la investigación de amenazas como el phishing, el malware, bandas de ransomware y mucho más.

Gracias a su conocimiento en primera línea, el Laboratorio desarrolla contramedidas eficaces contra ataques reales. Sus análisis detallados son la base de nuestras soluciones de ciberseguridad de próxima generación, que ayudan a las empresas a estar un paso por delante de los ciberdelincuentes.

TABLA DE CONTENIDOS

CYBERSECURITY
REPORT 2025

CAPÍTULO 1
RESUMEN EJECUTIVO

CAPÍTULO 1 – RESUMEN EJECUTIVO

Gracias al extenso conjunto de datos de usuarios de Hornetsecurity, se puede realizar un análisis detallado de las amenazas vinculadas al correo electrónico, así como al ecosistema de Microsoft 365 en general. Esto permite a los investigadores de seguridad convertir esos datos en información clave para los equipos de IT y los profesionales del sector. El correo electrónico sigue siendo uno de los principales canales de comunicación, especialmente en el ámbito profesional. En nuestro análisis de más de 55,6 mil millones de correos electrónicos en 2024, encontramos que el 36,9% se clasificaron como "no deseados". De estos, el 97,8% eran spam o fueron rechazados directamente debido a indicadores externos, mientras que el 2,3% se consideraron maliciosos.

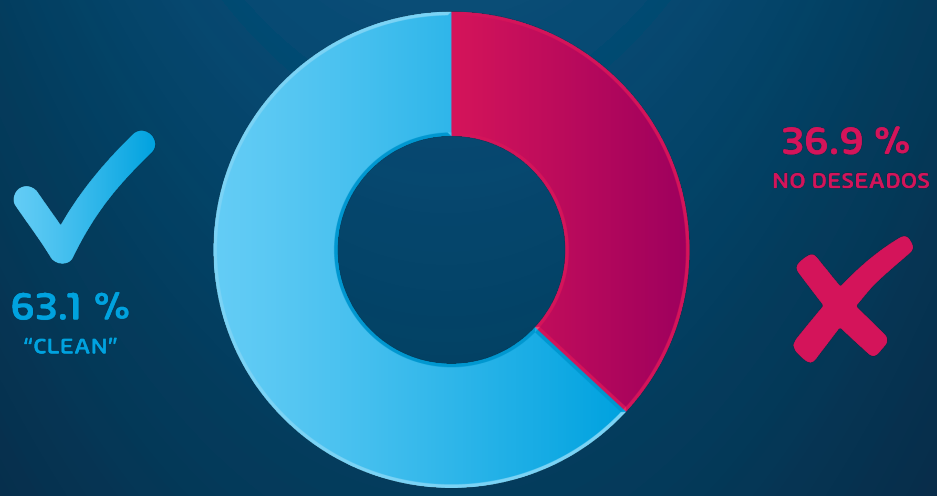


FIG 1. CLASIFICACIÓN DE CORREOS ELECTRÓNICOS ESCANEADOS POR HORNETSECURITY

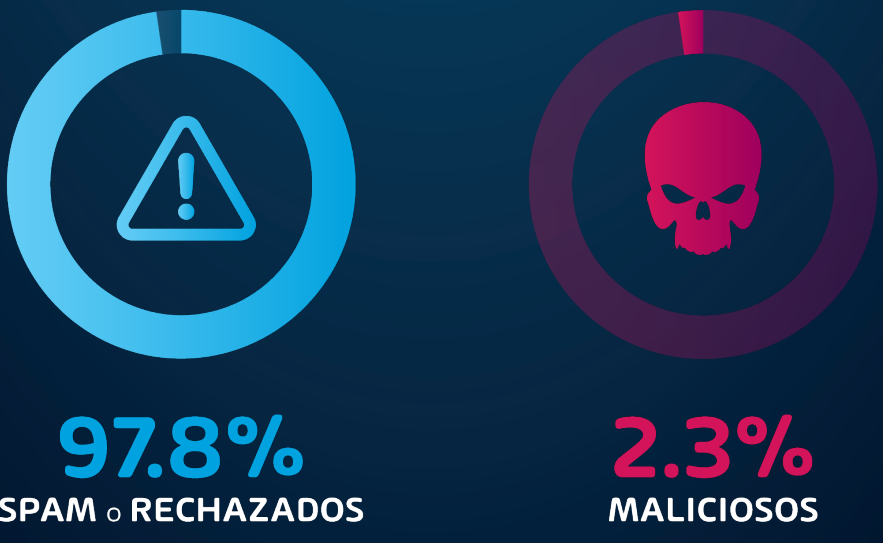


FIG 2. CLASIFICACIÓN DE CORREOS ELECTRÓNICOS NO DESEADOS

"PHISHING: 33,3% DE LOS ATAQUES"

Al evaluar los métodos de ataque más comunes en los correos electrónicos, el phishing se mantiene como el más prevalente, con un 33,3% de los ataques, seguido por enlaces maliciosos, que representan un 22,7%. Estas cifras reflejan las tendencias del último año, con un aumento de los ataques de robo de credenciales mediante proxys inversos, que se basan principalmente en técnicas de ingeniería social y el uso de enlaces engañosos.

Un enfoque renovado en la ingeniería social y el robo de credenciales también se hace evidente al analizar los tipos de archivos maliciosos empleados. Aunque ha habido una disminución general en el uso de archivos adjuntos maliciosos, los archivos HTML, PDFs y archivos comprimidos siguen siendo los tres formatos más utilizados, como ya se observó el año anterior.

Los atacantes han optado, en muchos casos, por incrementar ligeramente el volumen de correos más fáciles de detectar y, en consecuencia, de rechazar. Esto ha provocado una ligera disminución en el número de correos maliciosos clasificados como "Threats" y "AdvThreats". Como resultado, se ha registrado un descenso en el índice de amenazas en prácticamente todas las industrias. Aun así, el análisis sigue mostrando que todas las industrias son blanco constante de ataques, sin importar su sector. En lo que respecta a suplantación de marcas, observamos que, aunque DHL sigue siendo la marca más imitada, los intentos de suplantación de esta compañía han disminuido considerablemente. Por otro lado, los intentos de suplantación de FedEx se triplicaron, mientras que Docusign y Facebook duplicaron sus cifras. Mastercard y Netflix también experimentaron aumentos notables.

Por último, nuestra investigación sobre la seguridad en la nube destaca el creciente uso de kits para el robo de credenciales o tokens en ataques de tipo Adversario en el Medio. Estos ataques se han popularizado por su capacidad para dirigirse a un gran número de víctimas mediante páginas web muy convincentes y con un esfuerzo mínimo. A menudo, estos kits están diseñados para sortear sistemas de autenticación multifactor (MFA), lo que contradice la creencia de que este tipo de protección es completamente infalible. La industria de la ciberseguridad continúa trabajando para mitigar este problema mediante mejores herramientas de escaneo, formación en seguridad y tecnologías resistentes al phishing, como las claves de acceso. Sin embargo, la implementación de estas soluciones lleva tiempo, lo que deja a algunas organizaciones expuestas y con el riesgo de pérdida o filtración de datos sensibles.

Dado que este tipo de ataques sigue apoyándose principalmente en el correo electrónico, además de en plataformas de chat como Microsoft Teams, es imprescindible contar con una estrategia de seguridad robusta para protegerse en el entorno digital actual.

365 TOTAL PROTECTION

SABER MÁS

CYBERSECURITY
REPORT 2025

CAPÍTULO 2

EL PANORAMA ACTUAL DE AMENAZAS EN MICROSOFT 365

CAPÍTULO 2 – EL PANORAMA ACTUAL DE AMENAZAS EN MICROSOFT 365

Cada año, el Security Lab de Hornetsecurity se pone manos a la obra para revisar un gran número de datos de la empresa y analizar cómo está la situación en cuanto a amenazas globales relacionadas con el correo electrónico, además de estudiar estadísticas de comunicación. También desarrollan ejercicios de previsión para intentar adelantarse a posibles amenazas futuras. En este capítulo, nos centramos en el análisis de los datos recopilados entre el 1 de noviembre de 2023 y el 31 de octubre de 2024, que son la base para las proyecciones que se detallan en el Capítulo 4.

TENDENCIAS EN LA SEGURIDAD DEL CORREO ELECTRÓNICO

Aunque cada vez usamos más herramientas de colaboración y mensajería instantánea, como Microsoft Teams, el correo electrónico sigue siendo un blanco fácil para los ciberataques. Hemos visto cómo ha bajado el porcentaje de correos clasificados como "Threats" y "AdvThreats", pasando del 3,7 % del año pasado al 2,3 % este año. Si añadimos los correos "no deseados", en 2022 estábamos en un 5,5 %. Aun así, no podemos bajar la guardia, porque el riesgo para las empresas sigue siendo alto. ¿Por qué? Pues principalmente por el aumento de ataques de ingeniería social: correos masivos, con poco esfuerzo por parte de los atacantes, pero diseñados para que caigas en la trampa y hagas clic o interactúes.

Tras analizar más de 55.600 millones de correos electrónicos durante este período (del 1 de noviembre de 2023 al 31 de octubre de 2024), el laboratorio ha sacado algunas conclusiones clave:

SPAM, MALWARE Y MÉTRICAS DE ADVTHREATS

Como llevamos viendo desde hace más de una década, el correo electrónico sigue siendo la vía preferida de los atacantes para sus fechorías. Según los datos de este año, el 36,9 % de todos los correos electrónicos fueron clasificados como "no deseados", lo que supone un aumento de 0,6 puntos respecto a 2023. Cuando hablamos de "no deseados", nos referimos a esos correos que no interesan ni al destinatario ni a nadie. En el gráfico que sigue, se puede ver cómo clasificamos los correos no deseados frente a los correos limpios.

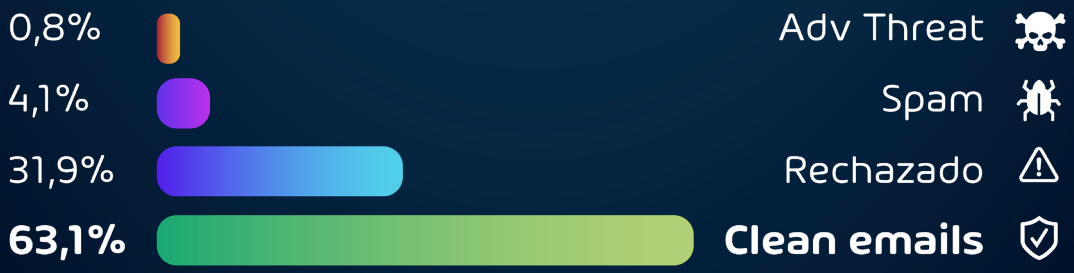


FIG 3. CORREOS ELECTRÓNICOS NO DESEADOS JUNTO CON CORREOS ELECTRÓNICOS LIMPIOS

El panorama de los correos electrónicos no deseados sigue dando de qué hablar. Este año, el 36,3% de todos los correos procesados se ha clasificado como "no deseados", lo que supone un ligero aumento respecto al año pasado. Si tenemos en cuenta que en 2024 se gestionaron 55.600 millones de correos electrónicos, esto significa que alrededor de 20.500 millones de esos correos fueron directamente a la categoría de "no deseados".

Para aclarar el panorama, aquí tienes un desglose de los tipos de correos electrónicos no deseados y cómo los clasificamos:

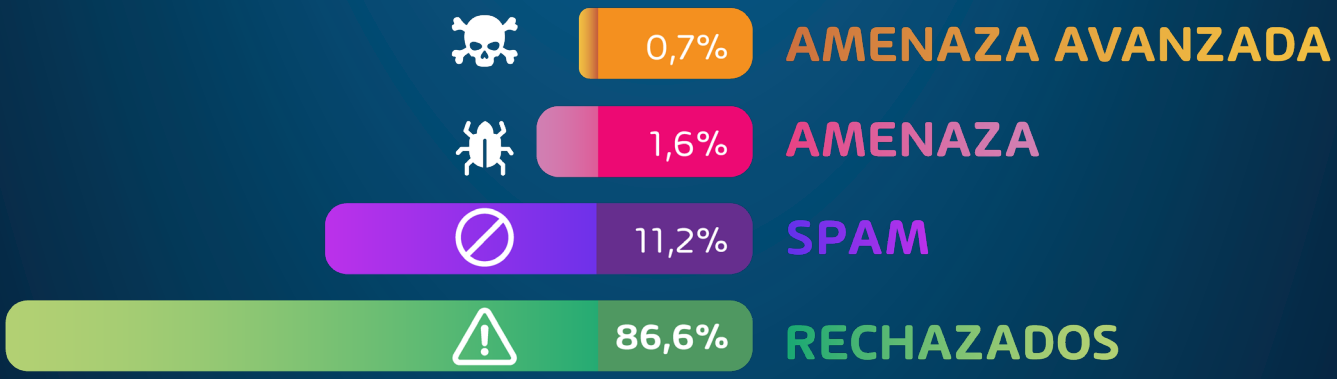


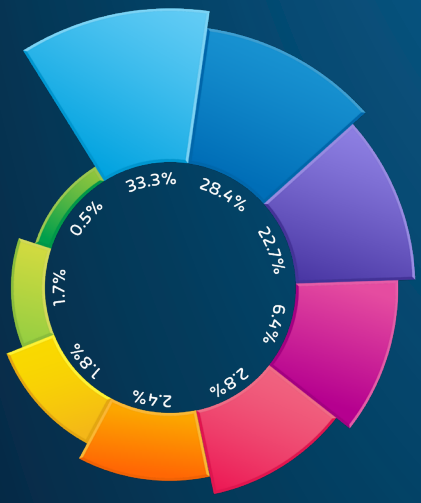
FIG 4. CORREOS ELECTRÓNICOS NO DESEADOS POR CATEGORÍA EN 2024

CATEGORY	DESCRIPCIÓN
Spam	Estos correos son los típicos que nadie quiere: promociones que no has pedido o mensajes fraudulentos. Se envían en masa, así que los recibimos miles de personas a la vez.
Amenaza	Este tipo de correos ya empieza a dar más miedo. Suelen llevar adjuntos peligrosos o enlaces maliciosos y están diseñados para engañarte y robarte datos, como en los casos de phishing.
Amenaza Avanzada	Aquí hablamos de correos más sofisticados, preparados para cometer delitos usando técnicas avanzadas. Solo pueden ser detectados y bloqueados con herramientas de seguridad muy punteras. Es el nivel pro de los correos maliciosos.
Denegados	Estos ni siquiera llegan a tu bandeja. El servidor de correo los rechaza directamente durante el primer intento de conexión. Esto ocurre porque el remitente parece ser poco fiable, ya sea por su dirección IP o por su historial.

NOTA: Cuando decimos que un correo ha sido "rechazado", nos referimos a que nuestro sistema, en este caso el de Hornetsecurity, lo bloquea durante el diálogo SMTP, antes de que entre en el sistema. Esto pasa cuando detectamos señales claras de que el remitente no es de fiar, como una mala reputación de su IP o una identidad comprometida. Es como si te intentaran vender algo puerta a puerta y tú cerraras antes de que empezaran a hablar.

TÉCNICAS DE ATAQUE POR CORREO ELECTRÓNICO EN 2024

En el análisis que hemos realizado de los correos electrónicos durante este año, hemos detectado la siguiente distribución de los tipos de ataques más comunes:



TÉCNICA DE ATAQUE	
PHISHING	33.3%
"OTROS"	28.4%
URLS MALICIOSAS	22.7%
ESTAFA DE PAGO ANTICIPADO	6.4%
EXTORSIÓN	2.8%
.EXE EN DISCO/ARCHIVO	2.4%
SUPLANTACIÓN DE IDENTIDAD	1.8%
HTML MALICIOSO	1.7%
MALDOC (DOCUMENTOS MALICIOSOS)	0.5%

FIG 5. TÉCNICAS DE ATAQUE POR CORREO ELECTRÓNICO EN 2024

NOTA: En años anteriores, podíamos comparar cómo evolucionaban los tipos de ataque de un año a otro. Sin embargo, este año hemos cambiado nuestra forma de identificar elementos maliciosos y correos no deseados. Esto ha hecho que un porcentaje significativo de ataques se clasifique como "Otros". Esta categoría incluye métodos que no encajan en las categorías principales que solíamos detallar. Por tanto, no tiene mucho sentido comparar directamente estos datos con los del año pasado.Lo que sí queda claro es que el phishing sigue siendo el rey, ocupando el primer puesto como el método más utilizado en ataques por correo electrónico. Le siguen muy de cerca las URLs maliciosas, que han ganado popularidad entre los atacantes. ¿Por qué? Pues porque son especialmente efectivas en ataques para robar credenciales mediante proxies inversos, usando herramientas como Evilginx.

Fuera de esto, las estafas de pago por adelantado siguen siendo bastante comunes entre los ciberdelincuentes, seguidas de cerca por la extorsión, que ocupa el cuarto lugar. La extorsión es especialmente preocupante, ya que cada vez vemos más casos en los que los atacantes primero se llevan datos sensibles antes de lanzar un ataque de ransomware en un sistema. Si la víctima decide no pagar (quizá porque han restaurado los datos desde copias de seguridad), los delincuentes amenazan con publicar esa información. Vamos, que te meten en un buen lío.

USO DE ARCHIVOS ADJUNTOS Y TIPOS EN ATAQUES

En 2024, los archivos adjuntos en los correos electrónicos siguen siendo una de las herramientas favoritas de los hackers para introducir software malicioso. Los atacantes no solo los usan para esconder malware, sino también para darle un aire más creíble a sus mensajes tramposos. Según el tipo de archivo adjunto, algunos filtros básicos de spam o antivirus ni siquiera llegan a detectarlos, lo que facilita ataques más sofisticados, como el llamado **HTML smuggling**.

De hecho, los archivos HTML maliciosos siguen siendo los reyes en este tipo de ataques, ocupando el primer puesto entre los archivos más utilizados en correos maliciosos.

La distribución de los tipos de archivos usados para enviar estas cargas maliciosas durante el período analizado se detalla aquí:

TIPOS DE ARCHIVOS	2023	2024
HTML	37.5%	20.4%
PDF	22.8%	19.2%
ARCHIVE	19.4%	17.6%
EJECUTABLE	3.5%	3.2%
EXCEL	3.2%	3.0%
WORD	3.0%	2.5%
ARCHIVO IMAGEN DISCO	2.2%	2.2%

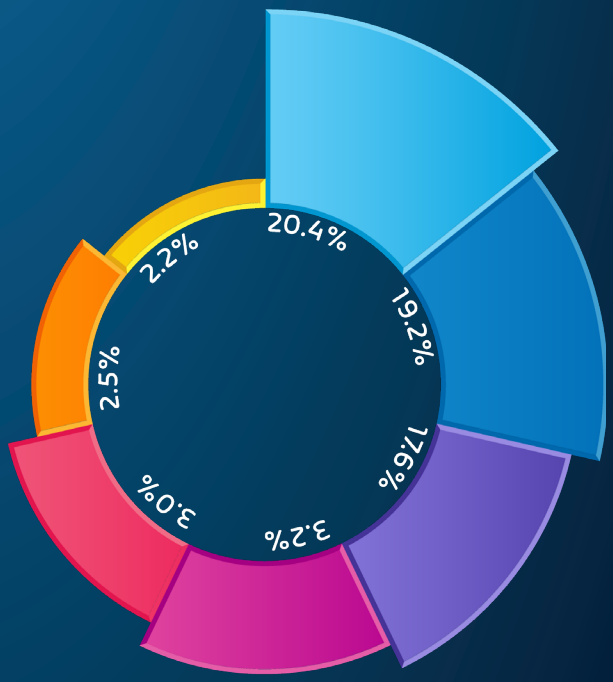


FIG 6. TIPOS DE ARCHIVOS PARA CARGAS ÚTILES MALICIOSAS EN 2024

> En 2024, se ha notado una caída de 17,1 puntos porcentuales en el uso de **ARCHIVOS HTML** respecto a 2023

- Los archivos PDF también han bajado, aunque menos, con una reducción de 3,6 puntos porcentuales.
- Algo parecido ha pasado con los archivos comprimidos, que han disminuido 1,8 puntos porcentuales este año.
- En general, estamos viendo un descenso casi total en el uso de archivos maliciosos de cualquier tipo. Los atacantes están cambiando de estrategia y apostando por otros métodos.

Durante el último año, los archivos adjuntos maliciosos ya no han sido tan efectivos como antes para los ciberdelincuentes. Por eso, ahora prefieren técnicas de ingeniería social para que la víctima haga algo diferente a abrir un archivo adjunto. Un ejemplo claro es el uso masivo de kits de herramientas de tipo "adversario en el medio" con proxy inverso, que se ha disparado en este periodo. ¿El motivo? Con la expansión de la autenticación multifactor (MFA), los atacantes se están centrando más en robar tokens de autenticación que en enfrentarse a los sistemas de MFA de las víctimas. Herramientas como Evilginx o PyPhisher están siendo clave para ellos, ya que obtener un token es mucho más fácil que superar las barreras del MFA.

ÍNDICE DE AMENAZAS POR CORREO ELECTRÓNICO PARA SECTORES EMPRESARIALES

Una de las áreas que revisamos cada año (y también mes a mes) es el número de amenazas dirigidas a los diferentes sectores empresariales. Esto nos ayuda a identificar si hay campañas específicas o ataques dirigidos a ciertos sectores. Además, proporciona información valiosa para que los líderes empresariales evalúen si están en mayor riesgo de sufrir ataques.

Lo más llamativo de los datos de este año es que **TODOS** los sectores empresariales han visto una bajada en su índice de amenazas por correo electrónico. Esto concuerda con los datos que mostramos anteriormente, donde ya señalábamos que la cantidad de correos clasificados como "Threats" y "AdvThreats" ha disminuido en comparación con el año pasado.

Ahora bien, hay sectores que, aunque menos, siguen siendo algo más atacados que otros.

- **Industria Minera** - Muchas empresas del sector minero se enfrentan desafíos similares a los de la industria manufacturera. Además, trabajan con materiales valiosos como los metales preciosos, lo que las convierte en un objetivo muy goloso para ciberdelincuentes que buscan extorsionar con ransomware.
- **Industria del Entretenimiento** - Empresas relacionadas con el juego, como casinos o plataformas de venta de entradas, se han vuelto un blanco por las enormes cantidades de dinero que manejan. Un ejemplo claro fue el ataque en 2023 a MGM y Caesars Entertainment, que detallaremos más adelante.
- **Manufactura** - Este sector tiene fama de ser un blanco habitual de **doble extorsión** para los ciberdelincuentes. La razón principal es el robo de propiedad intelectual, ya sea para venderla o para chantajear a las empresas. Además, el uso masivo de dispositivos poco seguros, como los del Internet de las Cosas (IoT) o los controladores programables (PLCs), hace que estas empresas sean un objetivo fácil para ataques que buscan interrumpir la producción o llevar a cabo extorsiones dobles.

A continuación, te dejamos una tabla con la calificación del índice de amenazas para los principales sectores empresariales.

FIG 7. ÍNDICE ANUAL DE AMENAZAS POR INDUSTRIA

NOTA: El porcentaje del índice de amenazas se obtiene con esta fórmula:

Porcentaje del Índice de Threats = (número de correos electrónicos maliciosos [Threats + AdvThreats]) / (número de correos electrónicos maliciosos [Threats + AdvThreats] + número de correos electrónicos limpios) × 100

Este cálculo no incluye los correos de spam ni los correos informativos.

Nota sobre la metodología

Las organizaciones, según su tamaño, reciben cantidades muy diferentes de correos electrónicos. Por eso, calculamos el porcentaje de correos electrónicos maliciosos en relación con el total (tanto maliciosos como legítimos) que recibe cada organización. Esto nos permite hacer comparaciones más justas entre ellas. Luego, calculamos la media de esos porcentajes para todas las organizaciones de una misma industria. Así obtenemos la puntuación final de amenazas de cada sector.

SUPLANTACIÓN DE MARCAS

La suplantación de marcas sigue siendo una de las técnicas de ataque más utilizadas en los correos electrónicos en 2024, afectando tanto a particulares como a empresas.

Un ejemplo llamativo es DHL. Esta empresa de transporte ha vivido un cambio radical en los intentos de suplantación de su marca. En 2024, la cantidad de intentos fue solo una pequeña parte de los registrados en 2023. Aun así, DHL sigue siendo la marca más suplantada, con FedEx pisándole los talones.

¿Por qué las marcas de transporte son tan atractivas para los atacantes? Pues porque encajan perfectamente en ataques de ingeniería social, como el phishing y el **smishing**.

Ambos tipos de fraude se parecen muchísimo a las comunicaciones reales de estas empresas, lo que facilita que usuarios menos precavidos caigan en la trampa y compartan datos personales o información de pago.

Otros datos relevantes en esta área:

- **FedEx y Facebook:** Los intentos de suplantación de estas marcas se han triplicado en el último año.
- **Docusign:** Los intentos han aumentado al doble en el mismo periodo.
- **Mastercard y Netflix:** También han visto un incremento considerable en los ataques.

Con los datos que hemos recopilado, aquí tienes un resumen de las marcas más suplantadas y cómo han cambiado año a año:

FIG 8. COMPARACIÓN ANUAL DE MARCAS SUPLANTADAS

NOTA: Los datos sobre la suplantación de marcas varían bastante según la región. Por ejemplo, hay varias marcas alemanas en esta lista debido a nuestra amplia base de clientes en Alemania.

Tras analizar 10.743.561 dominios activos que envían correos electrónicos en 2024, hemos detectado brechas importantes en la implementación de medidas de seguridad. Esto deja a muchas organizaciones con la puerta abierta a ataques de suplantación de marcas y falsificación de correos electrónicos.

> **SOLO EL 35,4%**
> HAN IMPLEMENTADO DMARC

Un dato preocupante: solo el 35,4% de los dominios analizados han implementado protocolos **DMARC** (Autenticación, Informe y Conformidad Basada en Dominios). Es decir, casi dos tercios de los dominios siguen sin esta medida crítica de protección. Además, apenas el 16,6% utiliza capacidades de RUA (URI de Informes Agregados), que son clave para obtener visibilidad sobre los resultados de la autenticación de correos electrónicos.

Los registros RUA son una pieza fundamental de DMARC. Gracias a ellos, los propietarios de dominios pueden recibir informes detallados sobre el uso de su dominio en correos electrónicos.

Estos informes incluyen información como:

- El volumen de mensajes recibidos.
- Las direcciones IP que envían correos en nombre del dominio.
- Las tasas de éxito o fallo en la autenticación.
- Las fuentes de envío y su cumplimiento con las políticas del dominio.

Entre los dominios que sí han implementado **DMARC**, el 47% utilizan las capacidades de RUA. Esto demuestra que muchas organizaciones que adoptan DMARC comprenden el valor de contar con monitoreo y visibilidad.

Gracias al monitoreo de RUA, las organizaciones pueden detectar aumentos de correos electrónicos falsificados que provienen de direcciones IP desconocidas. Esto les permite reaccionar rápido, por ejemplo, alertando a sus clientes sobre posibles campañas de phishing. En el caso de las instituciones financieras, este monitoreo resulta vital: les ayuda a iniciar procesos para eliminar amenazas en cuestión de horas desde que empieza una campaña de phishing.

SEGURIDAD DE LOS DATOS EN LA NUBE

La "nube" lleva entre nosotros más de una década, pero es ahora cuando estamos viendo cómo las empresas dan el salto a gran escala, migrando sus operaciones o incluso adoptando modelos 100% en la nube. Pongamos como ejemplo el almacenamiento de datos empresariales. Hace diez años, lo habitual era que las empresas contasen con algún servidor local para guardar sus datos más importantes.

Sin embargo, cada vez es más común que se aprovechen los servicios de almacenamiento en la nube para esta tarea. Plataformas como SharePoint Online y OneDrive para Empresa están ganando terreno, convirtiéndose en los sitios clave para almacenar datos, protegidos además con herramientas como Microsoft Entra. Por eso, la seguridad de los datos en la nube no es solo una prioridad para los usuarios de M365, sino para cualquier servicio en la nube en general. Aunque en este texto nos centraremos en Microsoft 365 y su ecosistema en la nube, muchas de las ideas que veremos también aplican a otros proveedores.

Las defensas básicas de la nube de Microsoft han mejorado con los años, pero no son infalibles. Cada vez más empresas están implementando medidas de seguridad avanzadas, como la autenticación multifactor (MFA) o la protección básica del correo a través de herramientas como Exchange Online Protection. Sin embargo, estas medidas a menudo se quedan cortas. Los ciberdelincuentes no paran de perfeccionar sus métodos, como lo demuestran claramente ataques del tipo Adversary-in-the-Middle (Adversario en el medio).

El panorama ha cambiado mucho, pero está claro que la ciberseguridad no se puede dar por sentada. Como se dice, "más vale prevenir que curar", y esto aplica más que nunca en el ámbito de los datos en la nube.

Claves de acceso y ataques de "Adversario en el Medio" (AitM)

Donde va el defensor, va también el atacante. Desde hace años, tanto en Hornetsecurity como en otras empresas centradas en la seguridad, hemos insistido en la necesidad de utilizar la autenticación multifactor (MFA) como un sustituto más seguro del típico dúo usuario y contraseña a la hora de iniciar sesión. Poco a poco, hemos visto cómo más personas adoptan diferentes tipos de MFA, desde mensajes SMS hasta llaves de seguridad físicas. Pero, claro, los ciberdelincuentes no iban a quedarse de brazos cruzados viendo cómo les fastidian el chiringuito. Han evolucionado para seguir sacándole partido a su "negocio".

Una de sus estrategias estrella es el uso de kits de phishing con proxy inverso, ya sean gratuitos o de pago. Estos kits les permiten crear señuelos muy convincentes en correos electrónicos para que la gente pique y haga clic en un enlace. Una vez que llegas a una página de inicio de sesión que parece de lo más legítima, introducen tus credenciales, y ahí empieza la trampa. Tus datos de usuario y contraseña se envían al sitio real, pero también acaban en manos del atacante. Cuando el sistema genera el mensaje de MFA, los kits permiten que tú introduzcas el código o apruebes la notificación como siempre, mientras ellos, en segundo plano, roban el token que emite el servicio de identidad (como Entra ID). Con ese token, el atacante puede iniciar sesión como si fueras tú. A este truco se le llama "Adversario en el Medio" o AitM.

La solución pasa por usar métodos de MFA resistentes al phishing. Aunque son más recientes y todavía no están muy extendidos, ya hay ejemplos como **Windows Hello para Empresas**, las llaves de hardware FIDO2 y las claves de acceso (**Passkeys**). Estas tecnologías bloquean la autenticación únicamente en el sitio web legítimo. Así, aunque te engañen para que entres en una página falsa, la tecnología no funciona porque detecta que la URL no coincide.

Eso sí, no todo es de color de rosa. Por ejemplo, Windows Hello para Empresas necesita hardware específico y solo funciona en Windows. Las llaves FIDO2, por su parte, son bastante caras, lo que limita su uso. Sin embargo, las claves de acceso tienen una ventaja importante: utilizan las mismas tecnologías que las llaves FIDO2, pero aprovechan el chip de seguridad de tu móvil, ya sea iPhone o Android. Así te ahorras comprar hardware adicional. Aunque su adopción aún es lenta, cada vez más servicios están empezando a ofrecer soporte para claves de acceso. Si eres el encargado de la seguridad en tu empresa, este es el momento perfecto para probarlas.

Con nombres como Microsoft Entra ID, Google Workspace, AWS o incluso Facebook ya aceptándolas, estamos seguros de que en menos de un año su uso se disparará.

Preocupaciones por la Dependencia Excesiva de Proveedores: ¿Un Riesgo para la Seguridad de los Datos en la Nube?

La dependencia excesiva de proveedores no es otra cosa que dejar en manos de un solo proveedor buena parte o incluso todas las funciones esenciales de un negocio. El problema de este enfoque es claro: si el proveedor tiene un contratiempo, ya sea de seguridad o de cualquier otro tipo, la empresa que depende de él se lleva el golpe.

Llevamos tiempo hablando de este tema en nuestros **Informes Mensuales de Amenazas** y en el podcast **The Security Swarm**. Una preocupación recurrente, sobre todo en lo que respecta a Microsoft, que no deja de ganar terreno en distintos sectores. Y esto, lejos de solucionarse, parece que irá a peor.

En el último año han surgido nuevos motivos de preocupación que han vuelto a poner el foco sobre este problema. Por ejemplo, un artículo **interesante publicado** en junio de 2024 destacó una serie de brechas de seguridad en Microsoft que merecen atención.

Te cuento un caso concreto: Andrew Harris, un exempleado de Microsoft, detectó una grave vulnerabilidad en Active Directory Federation Services (AD FS) y trató por todos los medios de solucionarla. Pero sus advertencias cayeron en saco roto. Mientras tanto, Microsoft estaba cerrando un contrato multimillonario con el gobierno de Estados Unidos para sus servicios en la nube, y el problema se dejó aparcado. Cuando Harris dejó la compañía en 2020, salió a la luz el ataque de SolarWinds, posiblemente el mayor ataque a la cadena de suministro de la historia. Aunque inicialmente el foco se puso en SolarWinds y su producto Orion, los atacantes rusos aprovecharon la vulnerabilidad de AD FS para moverse por las redes tras obtener acceso inicial.

Y todo esto ocurrió mucho antes de los informes del **Cyber Safety Review Board (CSRB)** o de que Microsoft lanzara la **Secure Future Initiative (SFI)**. Ahora, la gran incógnita es si el "nuevo Microsoft" será capaz de priorizar la seguridad sobre el desarrollo de nuevas funcionalidades. Algo que, seamos sinceros, no es tarea fácil para ninguna empresa que quiere mantenerse en la cresta de la ola.

Al final, cada organización debe decidir hasta qué punto quiere depender de un solo proveedor. Pero si tenemos en cuenta años de problemas de seguridad y el limitado alcance de la responsabilidad que Microsoft asume sobre los datos de sus clientes, la elección parece bastante clara.

¿De qué es responsable Microsoft?

Muchos se hacen esta pregunta: "Si Microsoft no se ocupa de mis datos ni de mi seguridad, ¿entonces de qué es responsable realmente?". Pues bien, la postura de Microsoft sobre este tema no ha cambiado en 2024. Para entenderlo bien, hay que echar un vistazo al famoso Modelo de Responsabilidad Compartida de Microsoft.

Lo esencial de este modelo es que deja claro que

> **"LA RESPONSABILIDAD SIEMPRE RECAE EN EL CLIENTE PARA:"**

- Información y datos.
- Dispositivos (ya sean móviles o PC).
- Cuentas e identidades.

Vamos, que te toca a ti garantizar la seguridad y protección de tu información. Microsoft, en este caso, se lava las manos. Por eso, a medida que más empresas migran a la nube, es clave que lo tengan en mente cuando diseñen sus estrategias de protección.

Hay otro tema importante que no podemos dejar pasar. Ya lo mencionamos en nuestro informe del año pasado, pero sigue sorprendiendo a muchos usuarios de Microsoft 365 (M365), así que merece la pena repetirlo. En 2023, Microsoft dio un giro importante sobre su postura respecto al uso de aplicaciones de respaldo con M365. En una conferencia, **anunciaron Microsoft 365 Backup**, un servicio para hacer copias básicas de seguridad en M365. Pero, ojo, lo relevante no es tanto el servicio en sí, sino el cambio de discurso. Antes solían decir: "No necesitas respaldar los datos en M365". Este cambio de rumbo ha dado que hablar, y muchos en la industria creen que hay dos motivos detrás:

1. **Microsoft ha reconocido, al fin, que depender solo de la retención de datos no basta para garantizar la seguridad en M365.**
2. **Microsoft también ha visto el filón en el mercado de los respaldos y quieren llevarse su trozo del pastel.**

Ambas razones tienen sentido, pero la segunda cobra fuerza al ver que también han lanzado una API de respaldo para proveedores... eso sí, de pago, como era de esperar. En cualquier caso, el mensaje está más claro que nunca: las empresas **SON** las responsables de proteger los datos que alojan en los servicios en la nube de Microsoft.

Las dificultades de gestionar múltiples tenants en la nube de Microsoft

Con el paso de los años, los servicios principales de la nube de Microsoft se han convertido en algo casi imprescindible, y muchas organizaciones se encuentran ahora con el reto de manejar varios entornos de Microsoft 365 al mismo tiempo. Esto es algo bastante común, sobre todo en empresas que han pasado por fusiones y adquisiciones, o si eres un proveedor de servicios gestionados (MSP) que lleva varios clientes. En cualquier caso, gestionar múltiples tenants de Microsoft 365 puede acabar siendo un auténtico dolor de cabeza.

El problema principal viene cuando esta carga de trabajo adicional empieza a afectar directamente a la seguridad de los datos en la nube. Seguro que tu organización tiene definidos unos estándares para mantener las mejores prácticas de seguridad y activar las funciones necesarias en los entornos de Microsoft 365 que administra. Pero, siendo realistas, muchos administradores se las ven y se las desean para imponer esos estándares y evitar errores o configuraciones incorrectas cuando se trata de varios tenants. Por la propia naturaleza de los servicios en la nube, una mala configuración puede ser la línea que separa una organización segura de un desastre de seguridad.

Por eso, la gestión de tenants se está volviendo cada vez más crucial para mantener a salvo los datos en Microsoft 365. Es verdad que Microsoft tiene una herramienta llamada Lighthouse, pero no es perfecta. Muchos MSPs opinan que se queda corta en funciones y escalabilidad. Por suerte, algunas empresas han sacado soluciones más completas para cubrir esta necesidad, como **365 Multi-Tenant Manager para MSPs de Hornetsecurity**. En un mundo cada vez más enfocado en la nube, la gestión y la gobernanza adecuadas son más importantes que nunca. Los equipos de liderazgo deben tener claro que estos desafíos no son tonterías, porque una mala gestión puede poner en jaque la seguridad de los datos en la nube. ¡Más vale prevenir que curar!

CYBERSECURITY
REPORT 2025

CAPÍTULO 3
UN REPASO A LOS PRINCIPALES INCIDENTES Y NOTICIAS DE CIBERSEGURIDAD DE 2024

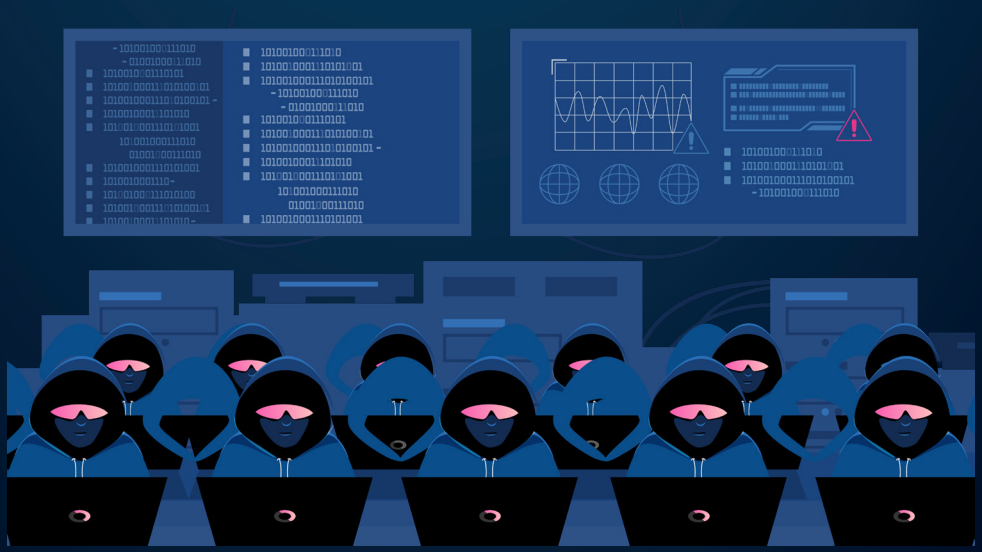
CAPÍTULO 3 – UN REPASO A LOS PRINCIPALES INCIDENTES Y NOTICIAS DE CIBERSEGURIDAD DE 2024

Este último año ha sido como una montaña rusa, con altibajos constantes en el mundo de la ciberseguridad. Si nos pusiéramos a enumerar todos los incidentes importantes, este informe sería el doble de largo. Así que vamos a centrarnos en los casos más destacados: los que han tenido mayor impacto o de los que podemos sacar buenas lecciones para proteger mejor nuestras organizaciones.

EL INCIDENTE DE CROWDSTRIKE

El 19 de julio de 2024 fue el día en que probablemente vivimos la mayor interrupción tecnológica de la historia. En un abrir y cerrar de ojos, cerca de 8,5 millones de sistemas Windows con el agente Falcon de CrowdStrike instalado sufrieron un fallo masivo: las famosas "pantallas azules". Los equipos entraron en un bucle de reinicios y bloqueos que sólo pudo solucionarse de forma manual. Este agente, que es una herramienta de Respuesta y Detección de Endpoints (EDR, por sus siglas en inglés), depende de un controlador del núcleo del sistema operativo, como suele pasar en Windows. Todo el problema comenzó por una actualización de firmas que contenía un error lógico. Este error hacía que se escribieran datos en una zona de la memoria que no debía tocarse, lo que provocó el desastre. El coste para las empresas afectadas, especialmente las de Fortune 500, se estima en más de 5.400 millones de dólares.

En septiembre, Microsoft reunió a los principales desarrolladores de ciberseguridad que trabajan con agentes para Windows en una cumbre global. El objetivo era buscar soluciones para evitar que algo así vuelva a suceder. Una de las ideas más comentadas fue que Microsoft adoptara un enfoque similar al de macOS: prohibir el acceso al núcleo y permitir solo interacciones a través de APIs. Sin embargo, este cambio tan radical no convence a todo el mundo, incluido nuestro equipo en Hornetsecurity. Creemos que limitar el acceso al núcleo podría frenar la innovación. Por ahora, Microsoft parece estar en la misma línea. Todo apunta a que las próximas versiones de Windows incluirán medidas de protección adicionales para reducir riesgos, pero sin llegar al extremo de cerrar por completo el acceso al núcleo.



CHANGE HEALTHCARE

En febrero de 2024, Change Healthcare, una filial de UnitedHealth, sufrió un ataque **masivo de ransomware** que puso patas arriba los registros personales, financieros y médicos de unos 100 millones de estadounidenses. Este ataque se atribuye al grupo de **ransomware BlackCat, con sede en Rusia**, y se considera la mayor brecha conocida de información sanitaria protegida en Estados Unidos. Los atacantes aprovecharon fallos en la red de la empresa para acceder a datos sensibles, como historiales médicos, detalles de seguros y datos de pago. Esta brecha no solo dejó al descubierto las carencias en ciberseguridad de Change Healthcare, sino que también sacó a la luz las debilidades del sector sanitario estadounidense en su conjunto.

Tras el ataque, Change Healthcare tuvo que ponerse las pilas para intentar reducir los daños, trabajando junto con las autoridades federales para investigar lo ocurrido. Sin embargo, la empresa no se libró del chaparrón: el público y los organismos reguladores no tardaron en exigir medidas más estrictas para proteger los datos en la industria sanitaria.

Lo más preocupante de este ataque es el **impresionante** impacto humano que tuvo. Por ejemplo, algunos pacientes en Estados Unidos no pudieron recibir a tiempo medicamentos esenciales. Algo parecido ocurrió con una brecha en el **NHS (Servicio Nacional de Salud) del Reino Unido**. Este tipo de ataques deja claro que a los ciberdelincuentes les importa bien poco a quién afectan con tal de obtener beneficio, llegando incluso a atacar al sector sanitario para aumentar sus posibilidades de cobrar un buen rescate.

VIOLACIÓN DE LOS DATOS PÚBLICOS NACIONALES

A principios de 2024, se produjo otra de las mayores brechas de datos de la historia: la **violación de los Datos Públicos Nacionales (NPD, por sus siglas en inglés)**. Hasta 2.900 millones de registros quedaron expuestos, afectando a unos 170 millones de personas en Estados Unidos, Reino Unido y Canadá. Entre los datos comprometidos había información de lo más delicada, como nombres completos, números de la Seguridad Social, direcciones postales, correos electrónicos y números de teléfono. El problema salió a la luz después de que un hacker accediera a los sistemas de la empresa en diciembre de 2023. Los datos estuvieron circulando por la dark web desde abril hasta el verano de 2024.

Las consecuencias de esta brecha son bastante serias. Los datos robados pueden usarse para todo tipo de fraudes y delitos cibernéticos. Las personas afectadas tienen ahora más riesgo de sufrir robo de identidad, transacciones financieras no autorizadas o ataques de phishing muy bien diseñados. Lo que hace especialmente grave este caso es que los atacantes podrían cruzar estos datos con otra información para llevar a cabo ataques de ingeniería social aún más convincentes.

BRECHA DE LOS CASINOS MGM Y CAESAR'S

A finales de octubre de 2023, justo cuando estaban cerrando los últimos detalles del informe del año anterior, tuvo lugar uno de los ciberataques más sonados del último año. Es imposible no mencionarlo aquí, ya que las consecuencias entran de lleno en el período analizado en este informe.

Los casinos y resorts de MGM y Caesar's fueron víctimas de un ataque de ransomware. MGM decidió no soltar ni un euro y calcula que recuperarse les costará alrededor de 100 millones de dólares. Por otro lado, Caesar's optó por pagar un rescate de unos 15 millones de dólares. Pero, ojo, la lección aquí no es que "si hay que pagar o no el rescate". Lo realmente importante es entender **cómo consiguieron entrar en primer lugar**: pura ingeniería social, machacando al personal de soporte técnico con todo tipo de tretas, incluido el soborno.

BRECHA EN EL SERVICIO DE PRUEBAS DE ADN DE 23ANDME

Lo que pasó con 23andMe es sorprendente. Durante meses intentaron minimizar el impacto de una **brecha en el servicio de pruebas de ADN de 23andMe**, pero en diciembre de 2023 tuvieron que reconocer que los datos de 6,9 millones de clientes habían sido robados (aunque, al menos, no publicados). Eso sí, los datos de un millón de usuarios de ascendencia judía sí acabaron filtrados en BreachForums, un foro de hackers que ya está cerrado. En aquel entonces, la autenticación multifactor (MFA) no era obligatoria, un fallo tremendo que ahora han corregido. Eso sí, el daño ya está hecho, y 23andMe tiene un problema financiero, en parte por esta brecha.

EL LÍDER DE LOCKBIT, DESENMASCARADO

En febrero de 2024, **la Agencia Nacional del Crimen británica logró hackear a los responsables de LockBit**, una de las bandas de ransomware más grandes del mundo, y desveló la identidad de su líder: Dmitry Yuryevich Khorosev. Pero aquí viene el quid de la cuestión: aunque logren identificar a estos delincuentes, las fuerzas del orden no pueden ni arrestarlos ni extraditarlos porque operan desde Rusia o países similares, donde las autoridades miran para otro lado siempre y cuando no toquen a sus compatriotas. En este contexto, el "doxeo" (revelar información personal de alguien) se convierte en una especie de revancha pública. La idea es ponerles la vida patas arriba: si otros criminales saben quién eres y dónde te escondes, no sería raro que se planten en tu casa a pedirte su parte. Al fin y al cabo, entre ladrones no hay honor, ¿no?

EL BACKDOOR EN XZ UTILS: UNA HISTORIA DE PELÍCULA

En marzo de 2024 salió a la luz otro caso digno de un thriller cibernético: el **backdoor de XZ Utils**. Aquí, un grupo de farsantes se ganó la confianza del encargado de este paquete de software de código abierto (OSS) durante años. Les ayudaron con mejoras en el código, revisaron documentación... Todo muy profesional. Pero claro, su objetivo final era asumir el control. Y cuando lo lograron, metieron una carga maliciosa que permitía colarse por la puerta trasera en conexiones SSH, siempre que se tuviera una clave especial.

Por suerte, esta versión comprometida solo llegó a las versiones alfa o de prueba de varias distribuciones de Linux. Fue Andrés Freund, un ingeniero de Microsoft, quien destapó el lío al detectar un uso extraño de la CPU mientras probaba un paquete de base de datos de código abierto. Ahora imagina el desastre si este ataque hubiera llegado a las versiones principales de Linux o a sistemas que dependen de SSH. Podría haber sido un auténtico caos. Aunque nadie se ha atribuido oficialmente el ataque, la mayoría de los expertos apuntan a los sospechosos habituales: espías rusos. La moraleja de esta historia es clara: si desarrollas software que dependa de componentes OSS (y en la mayoría de los casos, lo haces), no te olvides de evaluar su seguridad. Y no solo eso, sino también la de todo lo que se conecta con ellos.

UN AÑO COMPLICADO PARA MICROSOFT EN MATERIA DE SEGURIDAD

Microsoft no ha tenido precisamente su mejor racha en cuestiones de seguridad últimamente. De hecho, no les está yendo nada bien. En junio de 2023, el grupo chino Storm-0558 logró acceder a bandejas de entrada de correo electrónico de 22 organizaciones por todo el mundo, incluyendo nada menos que el Departamento de Estado de Estados Unidos. Se llevaron 60.000 correos electrónicos. Y no se quedó ahí. En enero de 2024, los rusos de Midnight Blizzard consiguieron colarse en buzones corporativos de Microsoft. Usaron técnicas de desfrizado de contraseñas para entrar en un entorno de prueba que contenía una aplicación OAuth con acceso al entorno de producción.

Este ataque no vino de la nada: fue un capítulo más en su historial, que incluye el lío de SolarWinds en 2020 y el hackeo de julio de 2021, donde también robaron información de algunos clientes. Por si no fuera suficiente, en marzo de 2024 repitieron la jugada, accediendo a sistemas internos y repositorios de código fuente usando credenciales robadas en el ataque de enero.

En abril de 2024, la Junta de Revisión de Seguridad Cibernética (CSRB, por sus siglas en inglés) publicó un **tercer informe** demoledor sobre el hackeo chino de 2023. Fueron directos: señalaron varios errores graves que facilitaron el ataque y propusieron 25 recomendaciones para evitar que vuelva a pasar.

Esta llamada de atención y los ataques en general han hecho que Microsoft se ponga las pilas y lance la Iniciativa de Futuro Seguro (SFI, por sus siglas en inglés). Al principio, muchos pensaron que era puro humo, un simple eslogan. Pero ahora resulta que incluye medidas serias, como evaluar anualmente el impacto en seguridad de todos sus empleados. Además, el nuevo lema de Satya Nadella es claro: "la seguridad es lo primero".

MANTENTE AL DÍA DE LAS ÚLTIMAS NOTICIAS DEL SECTOR

CYBERSECURITY
REPORT 2025

CAPÍTULO 4
PRONOSTICANDO EL PANORAMA DE AMENAZAS EN 2025

CAPÍTULO 4 – PRONOSTICANDO EL PANORAMA DE AMENAZAS EN 2025

¿ACERTAMOS CON LAS PREDICCIONES DEL AÑO PASADO?

Echar la vista atrás y revisar nuestras predicciones de la edición 2024 del Cybersecurity Report siempre resulta interesante. Anticipar lo que va a pasar nunca es fácil, y aunque acertamos en varias cosas, algunas otras no se desarrollaron como habíamos imaginado.

LOS RESCATES PAGADOS PRIMER SEMESTRE DE 2024 459 MILLONES DE DÓLARES

En 2024, hemos visto un aumento en los grupos de ransomware respecto a 2023. Hay más publicaciones en sitios de filtraciones, lo que confirma que este tipo de ataque sigue siendo una amenaza en auge. Las cifras hablan por sí solas: en 2023, los rescates pagados rondaron los 1.100 millones de dólares estadounidenses, mientras que las **estadísticas del primer semestre de 2024 ya van por los 459 millones de dólares estadounidenses.** Todo apunta a que 2024 será aún más "fructífero" para los ciberdelincuentes, con pagos más elevados debido a violaciones más graves, como el rescate récord de 75 millones de dólares que pagó una empresa del Fortune 50.

Ya esperábamos un aumento en los ataques de fatiga y bypass de MFA (autenticación multifactor), y efectivamente, esto se ha cumplido. La proliferación de herramientas, tanto de código abierto como "comerciales", para crear correos de phishing y configurar proxys que imitan páginas de inicio de sesión legítimas se ha disparado. Esto responde al mayor uso de opciones de MFA basadas en notificaciones push, que son vulnerables a estos ataques. ¿Qué puedes hacer? Implementar opciones de MFA resistentes al phishing, como Windows Hello para Empresas, claves de hardware FIDO2 o Passkeys, que utilizan un smartphone como clave sin necesidad de adquirir dispositivos adicionales. Estas tecnologías están "ancladas" a páginas de inicio de sesión legítimas, de forma que si te engañan para entrar a un sitio falso, simplemente no funcionan.

Hace tiempo identificamos riesgos en el antiguo cliente de **Microsoft Teams**, construido sobre la plataforma Electron. Afortunadamente, ahora lo han reemplazado por un cliente nuevo que parece tener menos vulnerabilidades. Eso sí, Teams sigue siendo un objetivo para el phishing. Aunque las opciones predeterminadas de seguridad han mejorado (como advertencias al recibir mensajes de nuevos usuarios), el uso de Teams como vector de ataque no ha crecido mucho.

El spyware y el malware en los móviles siguen dando guerra. La **Unión Europea** y **Estados Unidos han tomado cartas en el asunto** para frenar la expansión de proveedores y su uso en sociedades democráticas, tal y como se veía venir.

Como ya comentamos, los ataques contra interfaces de programación de aplicaciones (APIs) han aumentado en 2024 comparado con 2023 (se estima un aumento del 20% al 29%, según varias fuentes). Este tipo de ataque suele ser un "enemigo invisible", y por eso es tan popular entre los ciberdelincuentes. La vigilancia y las alertas para APIs no son tan potentes como las de otros sistemas. Si tu organización publica APIs para aplicaciones web de forma pública, asegúrate de tener un modelo de seguridad sólido y de estar atento ante usos malintencionados, como ataques DDoS.

Gestionar la ciberseguridad en los tenants de Microsoft 365 sigue siendo un hueso duro de roer, como ya advertimos. Dicho esto, queremos destacar una herramienta nueva que está en versión preliminar pública y disponible para todos los tenants de M365: **Exposure Management.** Esta herramienta te ayuda a la hora evaluar la configuración de seguridad y la postura de tu tenant. Además, te señala en qué deberías centrarte para mejorar puntos clave, como protegerte contra el compromiso de correos empresariales (BEC) o el ransomware.

El Tiempo de exploit (el período entre que se publica una vulnerabilidad y que aparece un exploit funcional) ha disminuido: de 63 días en 2018/2019, a 32 días en 2021/2022, y a tan solo 5 días en 2023. Aunque aún no tenemos cifras cerradas para 2024, ya hemos visto varios ataques exitosos a los pocos días de que se revelara una vulnerabilidad. Esto mete más presión a los defensores, porque parchear todo no es ni rápido ni fácil, y es imposible cubrirlo todo a la vez. Aquí es donde entra en juego la priorización: asegúrate de que los dispositivos expuestos a internet están bien actualizados.

Por otro lado, los dispositivos IoT siguen siendo el eslabón débil de las redes empresariales. Sólo en los **cinco primeros meses de 2024**, los ataques a estos dispositivos han crecido un 107% en comparación con el mismo período de 2023.

En cuanto a los deepfakes, este año hemos visto algunos que parecen sacados de una película de ciencia ficción, con herramientas de IA que generan imágenes, audio y vídeos bastante logrados. Aun así, no hemos tenido grandes brechas de seguridad a causa de ellos.

Eso sí, no hay que dormirse en los laureles: conforme estas herramientas sean más accesibles y avanzadas, es de esperar que proliferen los ataques y las campañas de desinformación basadas en este tipo de tecnología.

LAS PREDICCIONES DEL SECURITY LAB

Como cada año, el equipo de **Security Lab** de Hornetsecurity se pone manos a la obra para analizar el estado del sector, repasar nuestros datos, estudiar las tendencias de ataque y mucho más. Todo este trabajo tiene un objetivo claro: adelantarse a las amenazas que podrían afectar a las empresas y echar un vistazo a los posibles cambios que se cuecen en la industria. Aquí tienes nuestras predicciones para 2025.

SECURITY LAB CYBERSECURITY INSIGHTS & ANALYSIS

A nadie debería sorprender que muchas de estas predicciones giren en torno a la inteligencia artificial (IA). Es lo que está en boca de todos. Algunas de ellas se agrupan de manera bastante lógica, mientras que otras son un poco más específicas. Por eso, las hemos dividido y explicado con detalle a lo largo de esta sección.

Los LLM en manos de atacantes

El año pasado nos pusimos a analizar el auge de ChatGPT y otros modelos de lenguaje a gran escala (LLM, por sus siglas en inglés) y cómo han impactado la ciberseguridad, tanto para los atacantes como para los defensores. Aunque al principio se temía que los LLM pudieran crear código malicioso de forma impecable, la realidad ha sido otra. De hecho, las interfaces de chat con IA y otras herramientas automatizadas han resultado ser más útiles para los defensores que para los atacantes.

Según datos de Microsoft, hemos visto casos concretos de atacantes usando LLM. Por ejemplo, Forest Blizzard, un grupo respaldado por el Estado ruso, utilizó LLM para investigar tecnologías de satélites y radares, probablemente con el objetivo de apoyar la guerra en Ucrania. También lo usaron para tareas más prácticas, como manipular archivos. Por su parte, Emerald Sleet, de Corea del Norte, se dedica al phishing y emplea los LLM para entender vulnerabilidades conocidas y mejorar el tono y la redacción de sus mensajes de engaño.

Finalmente, Crimson Sandstorm, un grupo iraní vinculado a la Guardia Revolucionaria Islámica, ha recurrido a los LLM para ingeniería social, depuración de errores y desarrollo en .NET. Lo curioso de todo esto es que casi todo lo que hacen con los LLM se podría haber logrado con simples búsquedas en internet. Eso sí, con una diferencia importante: utilizar un LLM público deja un rastro que facilita a empresas como Microsoft sacar estas conclusiones. En pocas palabras, si estás usando un LLM público como atacante, estás fallando en lo básico de la seguridad operacional (OpSec). Vamos, que te estás delatando tú solo.

Los ataques contra los modelos de lenguaje como los LLM no dejan de aumentar. Por eso, MITRE ha creado **ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems)**, una herramienta diseñada para seguir de cerca los distintos tipos de ataques, algo parecido a lo que hace la matriz **ATT&CK** en el ámbito empresarial.

Con esto en mente, todo apunta a que en el próximo año la IA y los LLM estarán en el centro de muchas conversaciones sobre ciberseguridad. ¿Por qué? Pues por varios motivos:

1. La IA será cada vez más clave para el reconocimiento y la recopilación de información.
2. Los atacantes se apoyarán en la IA para elegir el mejor momento para lanzar sus ataques. Analizará datos y te dirá cuándo dar el golpe perfecto.
3. La IA potenciará casi todos los métodos de ataque. Desde el correo electrónico y las llamadas, hasta la ingeniería social.
4. Se usará para localizar vulnerabilidades en infraestructuras con una rapidez asombrosa. Identificar puntos débiles será pan comido.
5. Eso sí, también será una gran aliada para los defensores. Las herramientas basadas en IA seguirán mejorando para proteger sistemas y contrarrestar amenazas.

Deepfakes con IA para engañar y manipular: un reto a la vuelta de la esquina

El uso de tecnología deepfake en ataques de spear-phishing es una amenaza que va cogiendo fuerza, y no sería raro que en 2025 lo veamos como algo habitual. Los deepfakes permiten crear vídeos y audios tan realistas que parecen calcados de personas reales. Esta tecnología podría utilizarse para elaborar mensajes de phishing que sean tan convincentes que la gente acabe picando y revelando información sensible o realizando acciones que comprometan su seguridad.

Pero no solo afecta a la ciberseguridad. Los avances en deepfakes también representan un peligro serio para la opinión pública. Imagina un vídeo tan real que no puedas distinguir si es verdadero o falso, y que, además, esté diseñado para manipular ideas o difundir bulos. Esto ya ha ocurrido y seguirá siendo un recurso para quienes buscan desinformar. El resultado es claro: una pérdida de confianza en lo que vemos y oímos en internet.

Ataques a modelos de lenguaje: un nuevo frente de batalla

Los modelos de lenguaje extensos (LLM, por sus siglas en inglés), que ahora están en boca de todos, también tienen su talón de Aquiles. Son vulnerables a ciertos tipos de ataques como las inyecciones, el robo de datos o los llamados jailbreaks. En estos, los actores malintencionados manipulan los datos que recibe el modelo para confundirlo o extraer información que no deberían. Estas brechas ponen en riesgo no solo la seguridad, sino también la confianza que depositamos en estos sistemas. Y con lo dependientes que nos estamos volviendo de ellos, no es difícil imaginar que ciertos gobiernos u organizaciones les saquen partido para sus propios fines. Ya sea difundiendo desinformación, colando enlaces maliciosos o algo peor, el impacto de estas tácticas aún está por descubrir.

Casos Legales y Regulaciones por el Uso de la IA: Lo que Está por Venir

El uso de la inteligencia artificial (IA) está en boca de todos, sobre todo desde que herramientas como ChatGPT irrumpieron con fuerza en el mercado. Las dudas sobre legalidad, derechos de autor y propiedad intelectual llevan tiempo rondando cada paso de la evolución de la IA generativa. Dicho esto, parece que estamos llegando a un punto en el que los litigios por el uso de modelos como estos serán cada vez más frecuentes y con consecuencias más serias.

No sólo eso, también es probable que veamos a los gobiernos poniéndose manos a la obra para regular el uso de la IA. Seguramente, las primeras medidas se centren en la protección de datos personales, especialmente en regiones como la Unión Europea, que ya está marcando el camino con su Ley de Inteligencia Artificial (AI Act). Estas nuevas regulaciones no solo afectarán a los desarrolladores de IA, sino también a las empresas que quieran incorporar estas tecnologías en su día a día.

Nuevos Retos con los Marcos Regulatorios

En lo que respecta a normativas, la llegada de nuevos marcos como NIS2, DORA, CRA o KRITIS (este último exclusivo de Alemania) supondrá un quebradero de cabeza para muchas organizaciones. Aunque su objetivo es mejorar la ciberseguridad y la protección de datos, cumplir con estos requisitos no será precisamente una cosa hecha. Implementarlos exigirá un esfuerzo considerable y un buen puñado de recursos.

Además, la figura del responsable de cumplimiento dentro de las empresas cobrará más relevancia que nunca. Y ojo, porque cada vez más compañías exigirán a sus socios y proveedores que cumplan con las mismas normativas que ellas.

Esto no es casualidad: los ciberataques a las cadenas de suministro están siendo más habituales y devastadores. Si antes se daba por hecho que las empresas asociadas eran fiables, ahora se piden pruebas de que cumplen con los estándares regulatorios, y esto no va a cambiar a corto plazo.

Corrupción en la Comunidad de Código Abierto

Durante años, el software libre y de código abierto (FOSS, por sus siglas en inglés) se veía como un refugio seguro dentro de un panorama tecnológico lleno de riesgos. Sin embargo, la cosa ha cambiado. El caso de XZ Utils, que ya comentamos antes, junto con otras vulnerabilidades de renombre, ha dejado claro que esa percepción no era del todo real. Lo que ocurrió con XZ Utils nos mostró a un atacante que intentó colar modificaciones en un paquete de código abierto muy conocido, con la idea de lanzar un ataque masivo a la cadena de suministro. Por suerte, no lo consiguió, pero estuvo cerca. Con este nivel de sofisticación, no es descabellado pensar que lo intentarán con otros paquetes igual de importantes para la industria. Ya se ha observado un **aumento notable en la cantidad de paquetes maliciosos en el ámbito del código abierto, y lo que ha estado ocurriendo recientemente con el repositorio de software PyPi** quizá sea solo la punta del iceberg. Así que mucho ojo con lo que viene.

Predicciones Continuadas sobre la Informática Cuántica

Hace tiempo ya hablamos de una amenaza que, aunque no está a la vuelta de la esquina, asoma en el horizonte: la computación cuántica. Aún nos queda un trecho para ver un ordenador cuántico capaz de romper la criptografía actual (lo que se conoce como CRQC, por sus siglas en inglés), pero algunos expertos calculan que esto podría ocurrir para 2037, con un margen de ±5 a 20 años. Vamos, que no es ciencia ficción, pero tampoco algo para mañana. Eso sí, los avances en este campo no paran. Al día en que estas máquinas estén operativas se le llama el "Q-Day". Si tu empresa guarda datos sensibles cifrados que necesitas conservar más allá de la próxima década, más vale que empieces a darle vueltas al tema. ¿Por qué? Porque agencias como la NSA (y, seguramente, otras por ahí) ya están acumulando enormes cantidades de datos que ahora no pueden descifrar, pero que podrían ser un libro abierto en el futuro gracias a estos ordenadores cuánticos.

En Estados Unidos, el **NIST** ya **ha aprobado tres algoritmos de cifrado pensados para resistir la llegada de la computación cuántica:**

- **ML-KEM:** un mecanismo de encapsulación de claves basado en redes modulares.
- **ML-DSA:** un algoritmo de firma digital, también basado en redes modulares.
- **SLH-DSA:** un algoritmo de firma digital que usa hashes sin estado.

Además, parece que pronto habrá un cuarto estándar. Y aunque los nombres antiguos, inspirados en cristales kyber, eran más de frikis, los nuevos dejan más claro dónde debe usarse cada uno.

Microsoft tampoco se queda atrás. A través de su **programa Quantum Safe**, ha incorporado ML-KEM a su biblioteca criptográfica de código abierto SymCrypt (usada en Windows 10, 11, Server, Azure y Microsoft 365). Y en nada le seguirán ML-DSA y SLH-DSA.

El gran desafío de la informática cuántica está en conseguir escalar su capacidad. Para tener un ordenador realmente funcional, harían falta miles de cúbits físicos y una corrección de errores brutal para obtener cúbits lógicos fiables. Es decir, aún queda mucho camino por recorrer, pero no tanto como para relajarse. Por eso, si tu organización guarda datos sensibles que, por normativas, necesitas mantener cifrados durante más de 10 años, toca plantearte cómo actualizarlos con un algoritmo que sea seguro frente a la computación cuántica. Ahora que los estándares ya están definidos, no hay excusas para quedarse atrás.

Aumento en la Adopción de Lenguajes "Seguros para la Memoria"

El software lleva años arrastrando problemas de seguridad por culpa de la gestión de la memoria. Entre ellos, cosas como desbordamientos de búfer o errores al **usar memoria ya liberada** (lo que llaman use-after-free). Para solventar esto, la industria está empezando a pasarse a lenguajes "seguros para la memoria" como Rust o Swift. Estos lenguajes vienen con protecciones integradas que evitan muchas de las vulnerabilidades más comunes relacionadas con la memoria. ¿El resultado? Los desarrolladores tienen menos quebraderos de cabeza a la hora de escribir código seguro. Además, con la **posibilidad de que lleguen nuevas regulaciones** en el sector del software, es más que probable que el uso de estos lenguajes se dispare. No solo porque ayudan a hacer el software más seguro, sino también porque es mejor estar preparado para lo que pueda venir.

¿QUÉ NIVEL DE RIESGO TENDRÁ MI ORGANIZACIÓN EN 2025?

Pues bien, la respuesta sigue siendo muy parecida a la de otros años: si tu organización puede pagar un rescate o maneja información valiosa que pueda venderse con fines de lucro, **ERES** un objetivo claro. Los datos sobre amenazas por correo electrónico en la industria confirman que los ciberdelincuentes no se olvidan de ningún sector. Dicho esto, si tu empresa gestiona datos sensibles, está metida en el sector de defensa, trabaja con infraestructuras críticas o maneja propiedad intelectual de mucho valor, el riesgo sube todavía más. Vamos, que si estás en uno de estos casos, eres una prioridad absoluta para los ciberdelincuentes.

QUÉ DEBEN HACER LAS ORGANIZACIONES PARA DEFENDERSE

Comenzar con lo básico

Las organizaciones suelen caer en el error de reaccionar sólo ante amenazas concretas, comprando soluciones de seguridad específicas para cada área y enfocándose en la tecnología sin atender primero los fundamentos básicos de la seguridad. Sin embargo, la mayoría de las brechas de seguridad no ocurren por ataques ultra sofisticados o técnicas avanzadas, sino por fallos en aspectos básicos. Por ejemplo, muchas empresas no implementan autenticación robusta, como el uso de MFA (autenticación multifactor) con dispositivos resistentes al phishing. También es común que permitan contraseñas débiles, configuren a los usuarios como administradores locales en sus dispositivos o no formen adecuadamente a los empleados para evitar que caigan en trampas como enlaces maliciosos en correos electrónicos. Además, no probar las copias de seguridad para comprobar que realmente pueden restaurarse puede provocar un desastre si se sufre un ataque de ransomware. Por otro lado, descuidar las actualizaciones de seguridad (los famosos parches) puede ser igual de peligroso.

En resumen, cuida primero la higiene básica de la seguridad, que incluye tecnología, procesos y personas. Comienza con una mentalidad de Confianza Cero (Zero Trust):

- **Verifica todas las conexiones:** que un dispositivo esté gestionado no significa que sea 100 % seguro, y que un usuario se conecte desde una red conocida no asegura que no sea un atacante utilizando credenciales robadas.
- **Usa privilegios mínimos:** da a cada usuario e identidad sólo los **permisos** imprescindibles para desempeñar su trabajo. Además, revisa regularmente los permisos para evitar que acumulen más de los necesarios.
- **Asume que en algún momento te vulnerarán:** construye tus defensas tan sólidas como te permita tu presupuesto, pero no olvides preparar un plan para cuando las cosas fallen. Pregúntate: si un atacante compromete a un usuario, ¿cómo lo detectaremos? ¿Cómo podemos limitar su capacidad de moverse por el sistema?

Una lista más completa está disponible en los mandamientos de **Zero Trust del Open Group.**

La cultura gana a la estrategia

Transformar tu empresa en un negocio ciberresiliente no es algo que se haga de un día para otro. Requiere tiempo, esfuerzo y mucha perseverancia. No puedes convertir tu empresa en una fortaleza cibernética sin involucrar a todo el equipo y, sobre todo, sin ayudarles a entender cómo les afecta y por qué tienen que ser parte de la solución.

Por ejemplo, cuando pongas en marcha la autenticación multifactor (MFA, por sus siglas en inglés), asegúrate de que la dirección (el equipo ejecutivo o C-suite) den ejemplo. Es importante que tanto ellos como el consejo de administración entiendan por qué es necesario añadir esta "molestia" al proceso de autenticación. Este cambio cultural implica algo muy importante: entender que la ciberresiliencia no es cosa solo del departamento de IT o de seguridad. No puedes proteger lo que no conoces. Si, por ejemplo, el departamento de marketing lanza un nuevo sitio web o usa una solución SaaS para gestionar clientes potenciales sin avisar a IT o a seguridad, el riesgo lo asume marketing, no IT. Al final, cada decisión tecnológica o de procesos lleva consigo riesgos, y es esencial que estos se gestionen de forma transparente para que la empresa pueda tomar decisiones con cabeza.

Una lección clave para los equipos de IT y seguridad es aprender a hablar en el idioma adecuado: el de la gestión de riesgos. Si te pones a soltar tecnicismos y explicaciones complejas, perderás al resto del equipo en segundos. Pero si traduces esos cambios tecnológicos y de procesos al lenguaje del negocio, hablando de riesgos o incluso de oportunidades, conseguirás que todos remen en la misma dirección.

Eso sí, recuerda que un negocio ciberresiliente nunca es algo estático. Igual que otros riesgos empresariales (geopolíticos, económicos o de competencia), la ciberseguridad evoluciona constantemente. La empresa tiene que estar siempre aprendiendo y adaptándose. Un ejemplo reciente son las nuevas formas en que los atacantes están superando métodos "débiles" de MFA, ya sea con kits de herramientas que interceptan autenticaciones o con ataques de fatiga MFA. Por no hablar de la amenaza siempre presente de la ingeniería social. ¿Tu servicio de asistencia (helpdesk) sería más efectivo defendiendo tu empresa que el de Caesar's o MGM?

Una estrategia de seguridad equilibrada

Hoy en día, para enfrentarte a los retos del ecosistema de seguridad, es imprescindible que las empresas adopten un enfoque equilibrado. Esto significa tener en cuenta las amenazas avanzadas específicas de su sector sin descuidar las medidas de seguridad básicas, que deben estar perfectamente integradas.

Confiar únicamente en una herramienta o solución ya no basta. La clave está en una estrategia en varias capas que proteja tanto de los ataques más comunes como de las amenazas únicas de tu sector. ¿Cómo debería ser esta estrategia? Aquí te dejo algunas ideas:

- **Detección avanzada de spam/malware con análisis de comportamiento mediante ATP**, para blindarte frente a la constante avalancha de ataques por correo electrónico.
- **Formación en concienciación sobre seguridad para los usuarios finales**, para que identifiquen intentos de ingeniería social y ataques de spear-phishing.
- **Capacidades de respaldo y recuperación** para asegurar que tus datos, tanto los locales como los almacenados en la nube (por ejemplo, en Microsoft 365), puedan recuperarse fácilmente si sufres un ataque de ransomware.
- **Características de cumplimiento y gobernanza** que ayuden a proteger contra fugas accidentales de datos y garanticen que cumples con las normativas.

Ve un paso más allá

Todo lo anterior es solo el principio. La gestión de riesgos, las evaluaciones de proveedores y las formaciones son campos que están en constante evolución, igual que las normativas y los requisitos de seguridad. Sabemos que no todas las empresas pueden ser expertas en ciberseguridad, así que lo mejor es apoyarte en proveedores de confianza. Por ejemplo, es posible que tu equipo de seguridad sea experto en prevenir la pérdida de datos, pero tal vez no esté tan preparado para enfrentarse a ataques avanzados a través del correo electrónico. Trabajar con un proveedor especializado como Hornetsecurity te permitirá sumar su experiencia a la tuya. La ciberseguridad no es cosa de uno solo. Es un trabajo en equipo. Así que, si tienes dudas o quieres reforzar tu estrategia, no dudes en contactar con tus proveedores de confianza. Entre todos, podemos lograr un entorno más seguro.

365 TOTAL PROTECTION

NEXT-GEN MICROSOFT 365 SECURITY

BUSINESS

PLAN 1

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAIMERS

ENTERPRISE

PLAN 2

INCLUDES ALL BENEFITS OF PLAN 1

- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

ENTERPRISE BACKUP

PLAN 3

INCLUDES ALL BENEFITS OF PLAN 1 + 2

- AUTOMATIC BACKUP OF M365 DATA
- GRANULAR RECOVERY WITH END USER SELF SERVICE
- UNLIMITED STORAGE IN ONE ALL-INCLUSIVE FEE

COMPLIANCE & AWARENESS

PLAN 4

INCLUDES ALL BENEFITS OF PLAN 1 + 2 + 3

- SECURITY AWARENESS
- PHISHING & ATTACK SIMULATION
- ESI® REPORTING
- PERMISSION MANAGEMENT
- PERMISSION ALERTS
- PERMISSION AUDIT
- DMARC REPORTING & MANAGEMENT
- ENHANCED EMAIL REPUTATION & DELIVERY
- EASY DNS MANAGEMENT & OPTIMISATION
- AI RECIPIENT VALIDATION
- COMMUNICATION PATTERN ANALYSIS
- SENSITIVE DATA CHECK

PRUEBA GRATUITA

SOBRE LOS AUTORES

ESCRITO POR

Andy Syrewicze

Andy lleva más de 20 años dedicándose a ofrecer soluciones tecnológicas en distintos sectores. Está especializado en infraestructura, la nube y la suite de Microsoft 365.

Ha sido reconocido como Microsoft MVP en Cloud y Datacenter Management, un honor que solo alcanzan los mejores. Además, cuenta con el prestigioso título de VMware Expert, algo que no muchos pueden presumir.

Paul Schnackenburg

Paul empezó su carrera en IT cuando lo más puntero eran los procesadores 286 y el sistema operativo DOS. Hoy en día dirige Expert IT Solutions, una consultora de IT enfocada en pequeñas empresas en Sunshine Coast, Australia. También imparte clases de IT en una academia certificada por Microsoft.

Es un autor muy respetado en el ámbito tecnológico, conocido por sus artículos técnicos sobre temas como Hyper-V, System Center, nubes privadas e híbridas, y plataformas públicas como Office 365 y Azure.

Entre sus credenciales destacan las certificaciones MCSE, MCSA y MCT.

HORNETSECURITY
CSR2025

CAPÍTULO 5
RECURSOS

- https://attack.mitre.org/techniques/T1027/006/
- https://github.com/kgretzky/evilginx2
- https://www.techtarget.com/searchSecurity/definition/double-extortion-ransomware
- https://www.csoonline.com/article/569273/what-is-smishing-how-phishing-via-text-message-works.html
- https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/
- https://youtu.be/SScaV2PjFcg?si=Ivjyfnk7YmwUUnVh
- https://www.hornetsecurity.com/en/blog/category/threat-reports/
- https://www.youtube.com/watch?v=o3JFNaNES0Q&list=PLyKOQIbp_zWzsfkSUQ0F-Ved_0bZXts70W&index=13
- https://www.propublica.org/article/microsoft-solarwinds-golden-saml-data-breach-russian-hackers
- https://www.cisa.gov/resources-tools/groups/cyber-safety-review-board-csrb
- https://www.microsoft.com/en-us/trust-center/security/secure-future-initiative?mso-ckid=35a127b0490c698b23e234bd4819680d
- https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- https://techcommunity.microsoft.com/t5/microsoft-syntex-blog/welcome-to-microsoft-inspire-2023-introducing-microsoft-365/ba-p/3874887
- https://www.hornetsecurity.com/us/services/365-multi-tenant-manager/
- https://techcrunch.com/2024/02/29/unitedhealth-change-healthcare-ransomware-alphv-black-cat-pharmacy-outages/
- https://en.wikipedia.org/wiki/2024_National_Public_Data_breach
- https://cybernews.com/security/mgm-caesars-ransomware-attack-timeline/
- https://www.theverge.com/2024/9/13/24243986/23andme-settlement-dna-data-breach-lawsuit
- https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned
- https://en.wikipedia.org/wiki/XZ_Utils_backdoor
- https://www.cisa.gov/resources-tools/resources/CSRB-Review-Summer-2023-MEO-Intrusion
- https://www.bleepingcomputer.com/news/security/ransomware-rakes-in-record-breaking-450-million-in-first-half-of-2024/
- https://www.politico.eu/article/eu-commission-national-security-does-not-justify-spying-document/

- https://home.treasury.gov/news/press-releases/jy2581
- https://virtualizationreview.com/Articles/2024/03/25/exposure-management.aspx
- https://wca.org/security-attacks-on-iot-devices-surge-by-107-in-early-2024/
- https://atlas.mitre.org/matrices/ATLAS
- https://attack.mitre.org/matrices/enterprise/
- https://www.infosecurity-magazine.com/news/156-increase-in-oss-malicious/
- https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
- https://www.microsoft.com/en-us/security/blog/2023/11/01/starting-your-journey-to-become-quantum-safe
- https://techcommunity.microsoft.com/t5/security-compliance-and-identity/microsoft-s-quantum-resistant-cryptography-is-here/ba-p/4238780
- https://github.com/microsoft/SymCrypt
- https://en.wikipedia.org/wiki/Buffer_overflow
- https://en.wikipedia.org/wiki/Dangling_pointer
- https://securityboulevard.com/2024/10/eu-cra-good-intentions-impossible-requirements/
- https://pubs.opengroup.org/security/zero-trust-commandments/