Axyom

nº 01

Awware

El magazine de ciberseguridad para PYMEs y profesionales conscientes

Axyom

Foto de Marc Torrents. Nacido en Barcelona, 1988.
Partner de Axyom.

Edición nº 01, abril 2025
Editado por Axyom Cyber Partners, SL – Patrocinado por Axyom

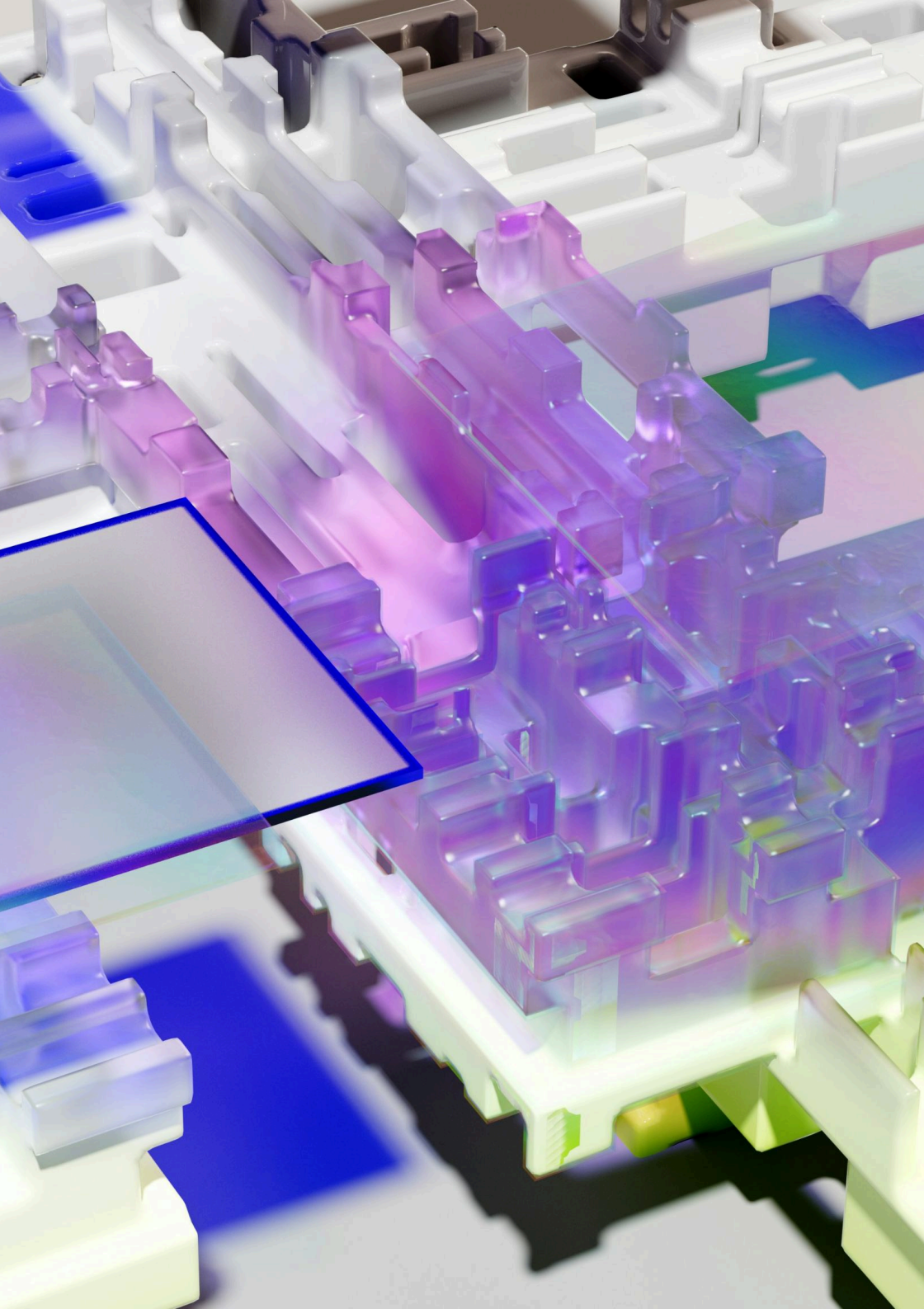
Editorial

Antes de nada, gracias por descargar este ejemplar de AWWARE, el magazine de ciberseguridad para PYMEs y profesionales conscientes. Con este primer número, iniciamos una andadura cuyo principal objetivo es poner a disposición de empresas, startups y profesionales los contenidos y herramientas sobre seguridad digital que hasta ahora solo estaban a disposición de las grandes corporaciones.

En Axyom sabemos que este vacío necesita llenarse, y las cifras lo confirman. Los ciberataques dirigidos a PYMEs han experimentado un crecimiento exponencial durante los últimos años y, a su vez, todas las previsiones apuntan a que las amenazas digitales no pararán de extenderse. Si a esto le sumamos que, tras un ciberataque, el 60% de las pequeñas y medianas empresas no sobreviven más allá de seis meses, es fácil hacerse una idea de la magnitud del problema.

Un problema que, además, representa una oportunidad, ya que las empresas que toman una posición de defensa activa ante estos riesgos se colocan un paso por delante de la competencia y añaden — en un mundo en que los datos son casi el principal activo de cualquier empresa — una importante capa de valor añadido para sus clientes.

Gracias a nuestros ciberseguros, contenidos especializados y herramientas de protección, queremos que cualquier empresa o profesional pueda dedicarse sin preocupaciones a su actividad. Axyom es tu partner de referencia para hacer frente a las ciberamenazas de hoy y del futuro. Esperamos que disfrutes de este primer número de AWWARE y que nos acompañes a lo largo de este emocionante camino.



Crime as a service

Cambio de paradigma. El crimen como servicio ha profesionalizado la ciberdelincuencia. Esto multiplica las amenazas para PYMEs y autónomos en un entorno digital cada vez más vulnerable.

Crime as a service: La democratización de la ciberdelincuencia y su impacto en las PYMEs

Si pensamos en ciberdelincuencia, probablemente la imagen que nos venga a la cabeza sea la de un hacker solitario encerrado en su habitación, estudiando líneas de código una a una y buscando la manera de penetrar en un sistema de la forma más elegante y discreta posible.

Pero eso ya no es así: ahora cualquier persona con intenciones maliciosas (y un poco de dinero), puede dotarse de las herramientas necesarias para ciberdelinquir. Este fenómeno, conocido como Crime as a Service (CaaS), ha transformado el panorama de las amenazas digitales, facilitando la entrada de actores no especializados en el mundo del cibercrimen.

¿Qué es el crime as a service?

En septiembre de 2024, una operación policial conjunta entre EUROPOL y AMERIPOL dio caza a una organización con presencia en varios países que se dedicaba a crear páginas web falsas con el objetivo de hacerse con los códigos de desbloqueo de móviles robados. De esta manera, se ponía fin a una infraestructura que había ayudado a mafias de todo el mundo a sustraer datos personales de casi 500.000 víctimas, que eran engañadas por medio de phishing y páginas web apenas distinguibles de las de Apple o Samsung en las que se les pedía el código de desbloqueo de su móvil para recuperarlo.

Seguir leyendo >>

El Crime as a Service se refiere a un modelo de negocio en el que delincuentes se ponen en contacto con proveedores de estos servicios, que diseñan soluciones a medida para que estas organizaciones puedan comenzar a ciberdelinquir sin conocimientos previos. Esta “profesionalización” del cibercrimen ha dado lugar a una industria donde se comercializan productos y servicios ilegales con estructuras similares a las de empresas legítimas, incluyendo soporte técnico y actualizaciones.

El ejemplo de la red desarticulada es solo una gota en el océano de una incipiente industria en la que es posible adquirir desde kits de malware y ransomware hasta servicios de plataformas de phishing o ataques DDoS (Denegación Distribuida de Servicio) por encargo.

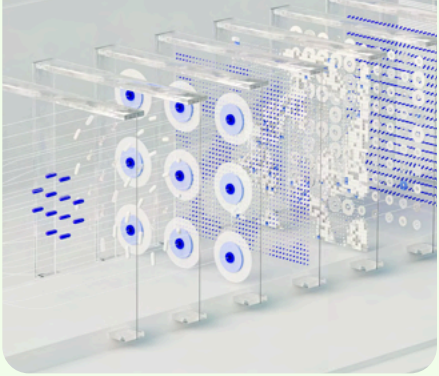
La reducción de la barrera de entrada al cibercrimen

El aumento imparable de los casos de cibercrimen tiene que ver, entre otras cosas, con el aumento de este tipo de servicios. Imaginemos una boutique a la que acceder mediante Telegram y que pusiera a disposición de cualquier persona malintencionada las herramientas necesarias para delinquir en Internet. Eso es exactamente el Crimen as a Service (Caas) y el resultado es que grupos sin experiencia previa pueden:

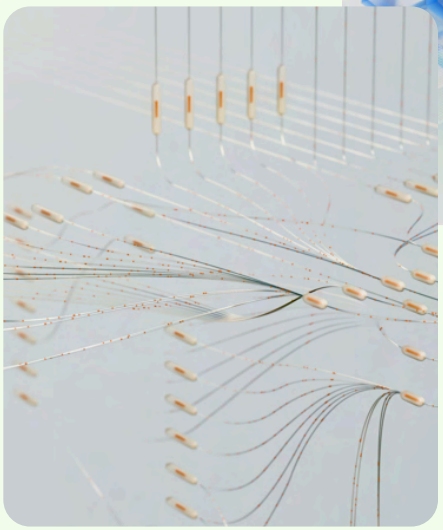
- **Adquirir kits de phishing personalizados:** A cambio de una suscripción, es posible obtener plantillas de correos electrónicos fraudulentos diseñados para engañar a las víctimas y obtener sus credenciales.

- **Comprar acceso a redes comprometidas:** Se venden accesos a sistemas ya vulnerados, permitiendo a los compradores infiltrarse en redes privadas sin esfuerzo.

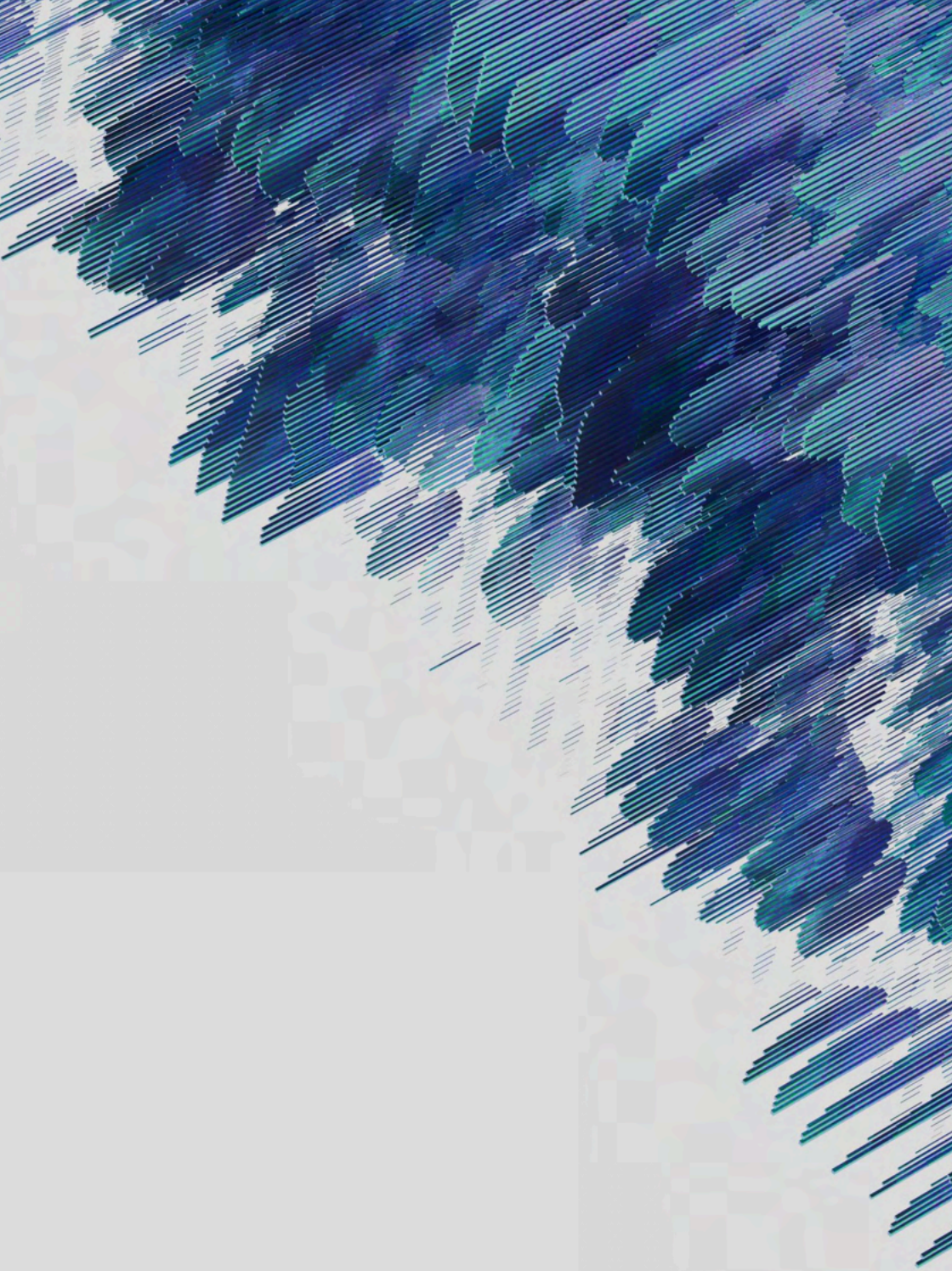
- **Contratar ataques DDoS:** También se pueden orquestar ataques que saturen y desactiven sitios web o servicios en línea de la competencia o de objetivos específicos.

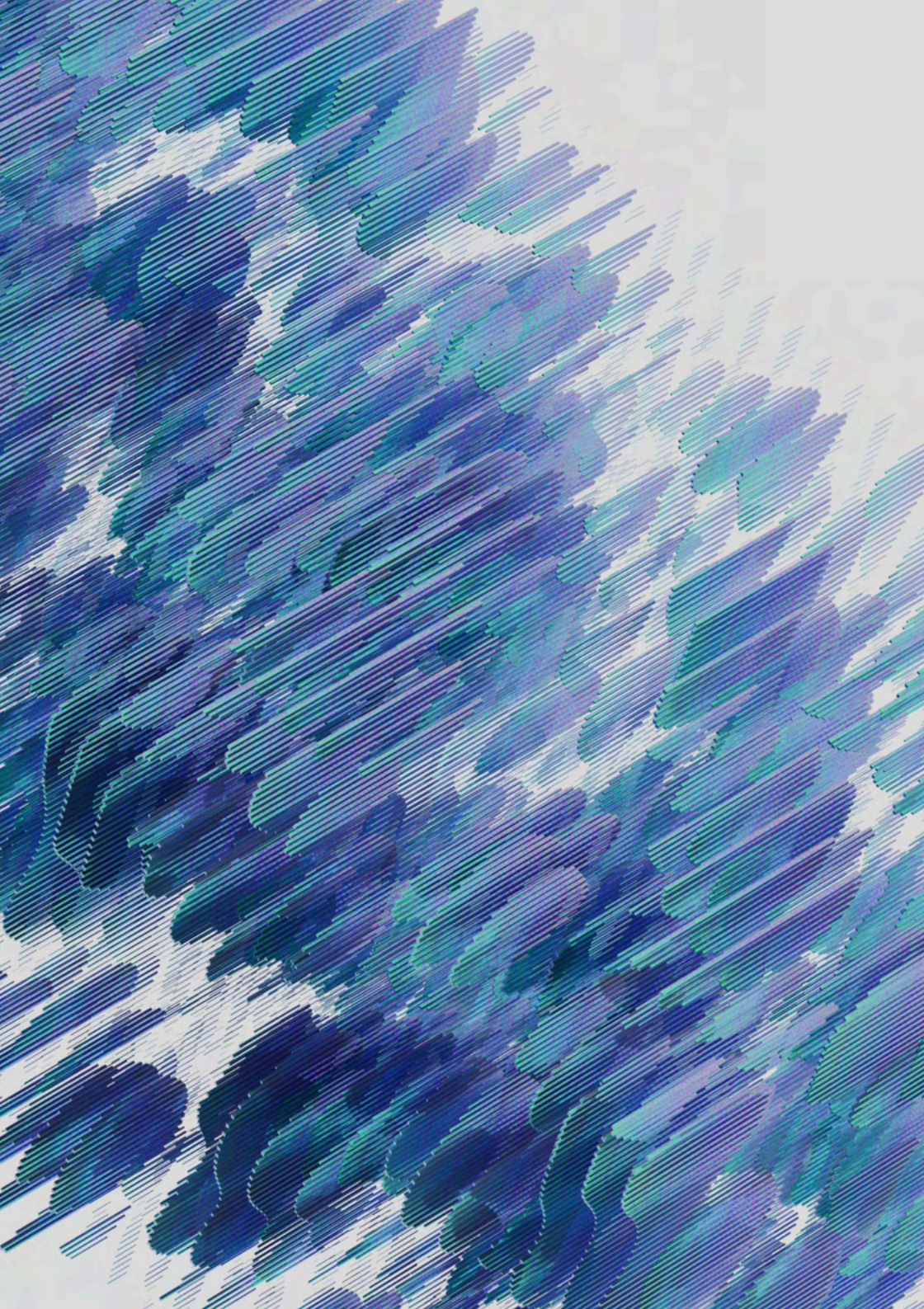


Cibercrímenes. El cibercrimen como servicio (CaaS) ha convertido el hacking en un negocio: por menos de 50€, cualquiera puede comprar kits de phishing o ransomware en la dark web.



El mercado de CaaS. Para 2026, se espera que el mercado de CaaS supere los 10.000 millones de dólares, impulsando un aumento exponencial en ataques a PYMEs y profesionales independientes.





El impacto en las PYMEs y profesionales

Si bien las grandes corporaciones cuentan con equipos especializados y un volumen de negocio suficiente para recuperarse tras un ciberataque, esto no es así en el mundo de la pequeña y mediana empresa. El dato es contundente: el 60% de las PYMEs colapsan antes de seis meses tras sufrir un ataque digital. Si a esto le sumamos el aumento imparable de estas amenazas gracias al Crimen as a Service, los riesgos se multiplican y se vuelven cada vez más dirigidos y personalizados, convirtiendo a las PYMEs en un blanco fácil.

Por ejemplo, en mayo de 2020, se detectaron campañas de phishing en las que los atacantes enviaban correos electrónicos que aparentaban ser de entidades como el Ministerio de Trabajo o la Seguridad Social. Estos correos informaban sobre inspecciones ficticias o pagos pendientes y tenían como objetivo pequeñas y medianas empresas de toda España. O más recientemente, en febrero de 2025, la Guardia Civil detuvo a 28 personas en Madrid y Toledo por estafar más de 82.000 euros a diversas víctimas, incluyendo dos empresas cántabras.

En ambos casos, los delincuentes se sirvieron de herramientas de terceros con el fin de conseguir rápidamente la infraestructura necesaria para realizar sus actividades ilícitas.

Medidas de protección para PYMEs y autónomos

Ante este panorama, es crucial que las PYMEs y los profesionales independientes adopten medidas proactivas para protegerse:

1. Formación para tus equipos. En Axyom siempre apostamos por la educación como medida fundamental para que nuestras PYMEs puedan desarrollar su actividad de forma segura. Transmitir a tus empleados una política clara respecto a las contraseñas, la autenticación o la gestión de correos electrónicos exteriores a la organización es clave para disminuir el riesgo de ser víctima de un ataque digital.

2. Actualización constante. Mantén todos los sistemas y aplicaciones al día con las últimas actualizaciones y parches de seguridad para minimizar vulnerabilidades. Asimismo, evita la utilización de webs no oficiales para la descarga de aplicaciones, así como la utilización de dispositivos de la empresa como el ordenador o el móvil para otros usos que no sean exclusivamente profesionales.

3. Hazte con un buen ciberseguro. Tanto en la fase de prevención como en la de recuperación, disponer de un ciberseguro es clave para minimizar los riesgos. Por ejemplo, en caso de robo de datos, un producto de este tipo puede ayudarte a recuperarlos y evitar así el riesgo reputacional para tu empresa. También puede cubrir las pérdida ocasionadas por la suspensión de tu actividad o proporcionarte asistencia técnica inmediata.

Ciberataques a PYMEs en 2024: Una amenaza creciente

#PYME #Ciberataques #OpenText

En 2024, las pequeñas y medianas empresas (PYMEs) han experimentado un incremento significativo en ciberataques. Según un informe de OpenText, el 76% de estas organizaciones fueron víctimas de ransomware, phishing y ataques a la cadena de suministro, poniendo en riesgo tanto sus operaciones como la seguridad de sus clientes.

Este aumento refleja la creciente vulnerabilidad de las PYMEs frente a las amenazas digitales y la necesidad urgente de fortalecer sus medidas de ciberseguridad.

Fuente: https://www.itdigitalsecurity.es/endpoint/2024/12/el-76-de-las-pymes-manifiestan-haber-sido-victimas-de-un-ataque-de-ransomware

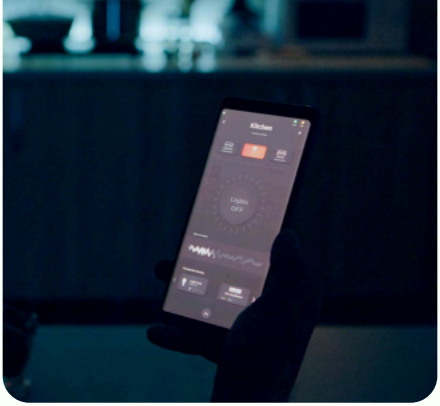
¡Hola! Soy tu banco: Estafa de phishing suplanta a CaixaBank para vaciar cuentas

#CaixaBank #Phishing

Los Mossos d'Esquadra han alertado sobre una nueva estafa dirigida a clientes de CaixaBank. Los delincuentes envían mensajes SMS que aparentan ser de la entidad bancaria, indicando una operación desde un nuevo dispositivo y solicitando verificar datos a través de un enlace fraudulento. Al acceder, los estafadores obtienen credenciales bancarias y vacían las cuentas de las víctimas.

En Axyom siempre recomendamos no hacer clic en enlaces sospechosos y contactar directamente con el banco ante cualquier duda.

Fuente: https://www.huffingtonpost.es/politica/lanzan-alerta-nueva-estafa-vaciarte-cuenta-caixabank-dan-regla-orobr.html

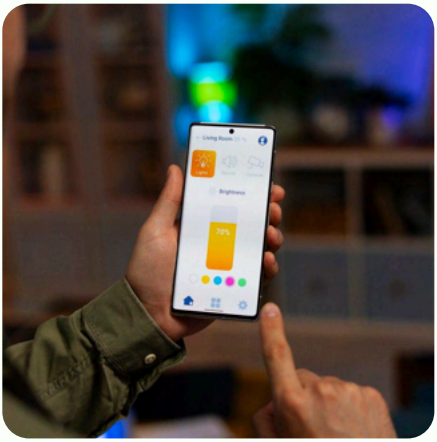


Por sus obras los conoceréis: Suplantación de voz del obispo de Segovia para estafar a sacerdotes

#Segovia #Suplantación #Tecnología

Un estafador ha clonado la voz del obispo de Segovia, Jesús Vidal, para engañar a varios sacerdotes de la diócesis. Haciéndose pasar por el obispo, solicitaba 2.200 euros para tramitar una supuesta herencia de 40.000 euros a favor de la diócesis. Aunque algunos clérigos fueron engañados, otros desconfiaron y alertaron a las autoridades. Este caso destaca el uso de tecnologías avanzadas para la suplantación de identidad y la necesidad de verificar siempre la autenticidad de solicitudes financieras inusuales.

Fuente: https://cadenaser.com/nacional/2025/02/26/un-estafador-suplanta-la-voz-del-obispo-de-segovia-para-intentar-robar-dinero-a-sus-sacerdotes-cadena-ser/



Descarga ahora: Empresa italiana distribuye software espía a través de aplicaciones Android

#Android #Software

Una investigación ha revelado que la empresa italiana SIO ha estado distribuyendo aplicaciones maliciosas para dispositivos Android durante años, disfrazadas de apps populares como WhatsApp. El spyware, denominado Spyrtacus, accedía a chats, contactos, registros de llamadas y controlaba micrófonos y cámaras. Aunque Google Play Store ha eliminado estas aplicaciones, se movieron a sitios web falsos de proveedores italianos. Se especula que Spyrtacus también podría tener versiones para iOS, Windows y macOS. En Axyom solo recomendamos descargar apps únicamente de fuentes oficiales, revisar opiniones y permisos solicitados.

Fuente: https://www.computerworld.es/article/2120245/una-empresa-italiana-de-software-espia-hackea-dispositivos-ios-y-android-segun-google.html

Entrevista a Martín Vigo

· Entrevista exclusiva para Axyom ·

Foto de Martín Vigo. Read Teamer e investigador en ciberseguridad. Conductor del podcast "Tierra de hackers" – Axyom Advisor.

“En ciberseguridad la educación es clave”

Martín Vigo es un destacado experto español en ciberseguridad, originario de Vilaxoán, Galicia. Su pasión por la informática comenzó a los 9 años, cuando recibió un ordenador Amstrad como regalo de Primera Comunión. Aquella pantalla monocromática, ideada para aprender a programar y correr videojuegos de 8 bits, despierta la curiosidad de Martín Vigo y, durante su adolescencia, comienza a interesarse por su verdadera pasón: la ciberseguridad y el hacking.

Tras pasar por empresas como Apple, Google y Salesforce, Martín Vigo funda Triskel Security, una consultora especializada en soluciones de seguridad de la información. Dirige el podcast “Tierra de Hackers”, donde analiza noticias y tendencias relacionadas con el hacking, las ciberamenazas y la privacidad en Internet. Y también es advisor de Axyom, donde ayuda a generar las mejores productos de ciberprotección para PYMEs.

Seguir leyendo >>

Martín, ¿cuál es la principal ciberamenaza que enfrentan a día de hoy las PYMEs?

En el caso de las PYMEs, lo más frecuente son ataques por medio de ingeniería social o phishing. Se trata de estrategias dirigidas a engañar directamente al usuario para que comparta sus credenciales. Esto es aún más peligroso si saltamos a lo que se conoce como spear phishing, en la que los ataques están totalmente customizados para engañar a personas específicas dentro de la organización.

¿Cómo logran los ciberdelincuentes este nivel de personalización en sus amenazas?

Es relativamente fácil a partir de la investigación. Basta con estudiar las redes sociales de la victima para idear un pretexto creíble. Por ejemplo, con el Linkedin scraping, el atacante puede averiguar el lugar de trabajo o los nombres de los compañeros de la víctima. Es bastante conocida la estafa del CEO, en la que por medio de Inteligencia Artificial se puede suplantar la identidad del responsable de la organización en un correo electrónico y pedirle a determinados empleados que realicen una tarea comprometedora, como una transferencia bancaria o la descarga de un archivo.

¿Qué es el perímetro de seguridad?

Imaginemos una frontera que delimita el interior del exterior de una empresa. El perímetro sería todo lo que queda dentro de esa frontera.

Sobre ciberataques a PYMEs. En el caso de las PYMEs, los ataques por medio de ingeniería social son uno de los principales riesgos.

Si un atacante quiere comprometer este perímetro, debe buscar una brecha de seguridad en los sistemas de la empresa que están expuestos hacia afuera. Esto normalmente lleva mucho tiempo de trabajo y equipos dedicados. Este tipo de amenaza es más propia de grandes corporaciones y gobiernos.

Al final, se trata de encontrar un agujero en un muro, lo cual es difícil. Por eso los ciberdelincuentes prefieren usar técnicas de ingeniería social

Y aquí debemos poner el foco en las personas que trabajan en esa empresa y sus actividades, es decir, todo lo que el ciberdelincuente puede hacer para comprometer la seguridad de la empresa engañando a esas personas.

Una sensación frecuente es que hay una auténtica industria relacionada con la ciberdelincuencia.

Sí, y acuña el término del CaaS, esto es, el cibercrimen como servicio. Por ejemplo, hace poco salió a la luz el caso de una persona en Argentina que se dedicaba a crear páginas web de Apple falsas con el fin de robar las contraseñas de los móviles robados.

Sobre ciberdelincuentes. El CaaS ha eliminado en gran parte la barrera de entrada para los ciberdelincuentes.

En este caso, distintas organizaciones dedicadas a robar móviles y mandarlos a Marruecos o China se servían de la infraestructura de esta persona para lanzar mensajes haciéndose pasar por Apple en los que se solicita el pin del móvil para recuperarlo. Una vez que el responsable de la infraestructura conocía el código de desbloqueo, se lo mandaba a sus "clientes" para que así pudieran resetear el móvil y venderlo.

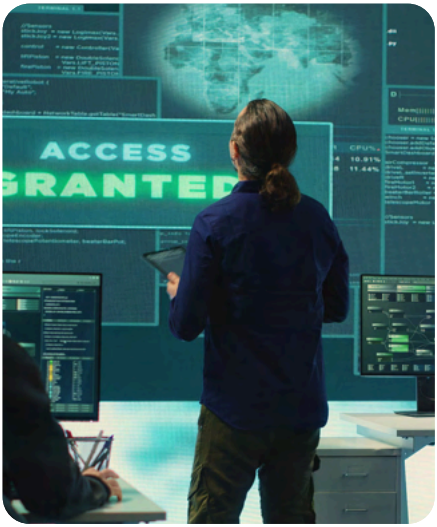
Esto sen realiza a escala industrial, con equipos perfectamente jerarquizados en los que se manejan KPIs, incentivos, programas de referal...

El resultado son palés enteros de móviles robados que viajan a estos países y un modelo de negocio que genera muchísimos beneficios para los delincuentes.

¿Qué es lo primero que debe hacer una pequeña empresa que quiera defenderse de estas amenazas digitales?

Lo principal es la educación. Al final estamos hablando de buenas prácticas en el trabajo y para eso es fundamental formar a los trabajadores. Por muchas barreras tecnológicas que pongas, si al final, por medio de un engaño, un empleado proporciona sus credenciales, poco más podemos hacer. Por este motivo, lo primero que debe de hacer una PYME para protegerse es marcar unas líneas de trabajo claras para toda la organización.

Sobre la importancia en la educación. La educación es clave para prevenir fallos de seguridad en los equipos de trabajo.



Sobre ciberataques. Para minimizar daños, hay que actuar antes, durante y después del ciberataque.

A esto podemos sumarle soluciones tecnológicas como un gestor de contraseñas o accesos a través de Google, por ejemplo, donde no son necesarias. Si además de esto utilizas una base de datos que impida la reutilización de contraseñas o implantas un sistema de doble autenticación, estás poniendo más barreras a los posibles ciberdelincuentes.

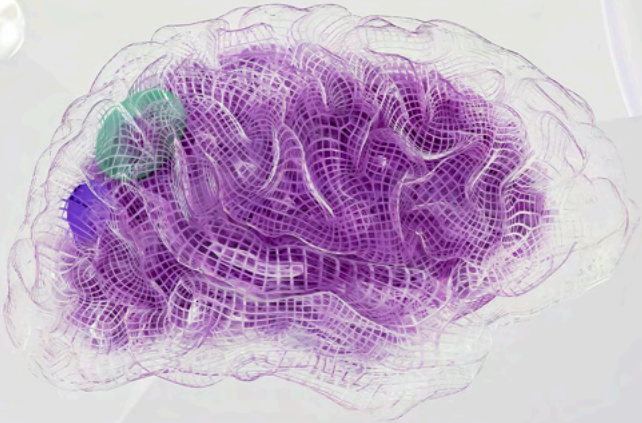
Por último, una buena política de recuperación en caso de ciberataque. El principal riesgo al que se enfrenta una PYME que ha sido hackeada es la interrupción de su negocio y el daño reputacional. Si tenemos claro qué hacer en ese caso y tenemos protocolos de actuación, es más sencillo recuperar la actividad de la empresa y disminuir el impacto.

Qué es más seguro, ¿Apple o Windows?

Hay algunas diferencias, pero ninguna es sustancial. Hoy en día los principales sistema operativos son perfectamente seguros.

Es posible que antes Windows estuviera un paso por detrás, pero a día de hoy están igualados. Pero volvemos a lo mismo: por muy seguro que sea un sistema operativo, si al final un empleado proporciona sus contraseñas a un ciberdelicuente, no existe forma de evitar el ataque. Por eso, como hemos dicho, la prevención y, más concretamente, la educación son claves.

Buenas prácticas en ciberseguridad. Las buenas prácticas en ciberseguridad son tan importantes como un sistema operativo seguro.



Ciberseguridad para PYMEs

Todo lo que siempre quisiste saber sobre ciberseguridad para PYMEs y nunca te atreviste a preguntar

En un mundo repleto de amenazas digitales, los hackers están situando su punto de mira sobre las PYMES, startups y profesionales. ¿La razón? Muy sencilla: los ciberseguros, conocimientos especializados y herramientas proactivas de protección solo han estado al alcance de las grandes corporaciones. Hasta ahora. Te explicamos las principales amenazas digitales a las que se enfrenta tu negocio, por qué existe Axyom y todo lo que vamos a hacer para cambiar las reglas del juego.

El paisaje actual de amenazas digitales (y el que vendrá)

Imagina que estás en tu oficina, tomando un café y comenzando la mañana. De repente, recibes un correo de un proveedor de toda la vida. O eso parece. Te pide que hagas clic en un enlace para revisar una factura. Todo normal, ¿no? Pero detrás de ese correo, podría haber un ciberdelincuente esperando a que hagas clic para robar tus datos o bloquear tus sistemas. Esto es lo que llamamos un ataque de phishing, y es solo una de las muchas amenazas que las pymes enfrentan cada día.

El phishing puede ser muy sofisticado. Los hackers son verdaderos artistas del engaño. Es extremadamente fácil caer en la trampa. Pero ésta no es la única amenaza. Imagina ahora que un día enciendes tu ordenador y ves un mensaje que dice que todos tus archivos han sido encriptados. Pedidos, datos personales, facturas. Todo. Y la única forma de recuperarlos es pagando un rescate en criptomonedas. Esto es ransomware, y puede paralizar completamente tu negocio, especialmente si no tienes copias de seguridad o un plan de respuesta a incidentes.

Ciberamenaza	Descripción	Repercusión en la PYME
Phishing y suplantación de identidad	Engaños para obtener información confidencial o realizar transacciones fraudulentas.	Pérdida de datos, acceso no autorizado, daño a la confianza de clientes.
Ransomware	Cifrado de datos y solicitud de rescate para su liberación.	Paralización operativa, pérdidas económicas, daño reputacional.
Malware	Programas maliciosos que dañan sistemas o roban información.	Pérdida de datos, compromisos de seguridad, disminución del rendimiento.
Ataques de Denegación de Servicio (DDoS)	Sobrecarga de recursos, impidiendo acceso a servicios.	Caída de servicios, interrupción de operaciones, pérdidas financieras.
Ingeniería social	Manipulación para obtener acceso o información.	Divulgación de información sensible, acceso no autorizado.
Ataques a la cadena de suministro	Compromiso de proveedores para infiltrarse en la empresa.	Interrupciones operativas, compromisos de seguridad, riesgos legales.

Otra amenaza creciente es el malware, que no es otra cosa que un virus informático de toda la vida. Estos programas se introducen en tus sistemas sin que te des cuenta y pueden causar todo tipo de daños: desde robo de información al compromiso total de toda tu infraestructura digital. Para una gran corporación, estos ataques son problemas graves, pero pueden hacerles frente gracias a sus recursos especializados en ciberseguridad. Sin embargo, para una PYME, un ataque puede ser devastador. Puede detener tus operaciones cotidianas, generar una imagen de desconfianza entre tus clientes y, en muchos casos, suponer el cierre de tu negocio.

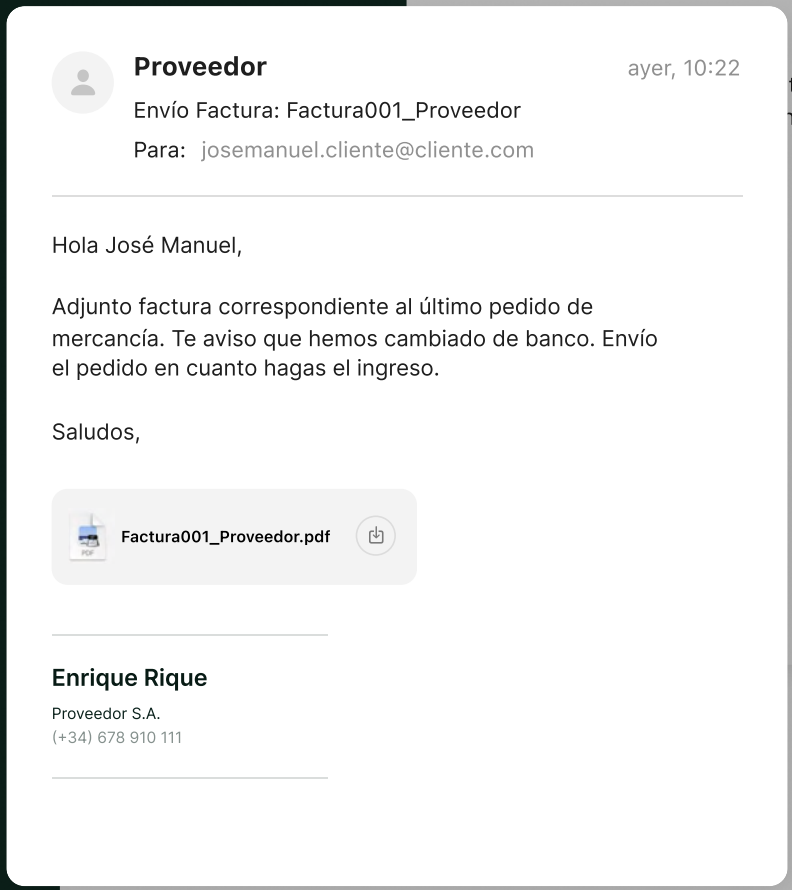
Pero si te contamos todo esto, no es para que vivas con miedo. Al contrario, la misión de Axyom es que, por medio de nuestros productos aseguradores, herramientas y contenidos, puedas estar preparado. Piénsalo de este modo: la ciberseguridad no es un lujo, sino una necesidad en nuestro mundo digital. Y para una PYME, startup o profesional independiente, los riesgos se multiplican si tenemos en cuenta sus características específicas.

¿Por qué las PYMEs son especialmente vulnerables a los ciberataques?

Para ilustrarlo, nada mejor que un caso real de Business Email Compromise (BEC), donde los ciberdelincuentes suplantan identidades corporativas para desviar fondos.

Una mañana cualquiera, José Manuel, contable en una pequeña empresa española, recibió un mensaje de Enrique, un proveedor de maquinaria habitual. En el correo, Enrique le adjuntaba algunas facturas pendientes y le pedía que actualizara los datos bancarios para realizar el pago, ya que a partir de aquel momento utilizarían otro número de cuenta.

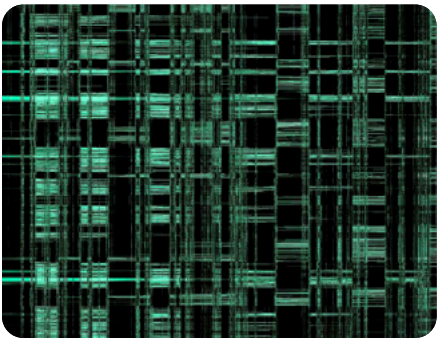
Seguir leyendo >>


Proveedor
ayer, 10:22
Envío Factura: Factura001_Proveedor
Para: josemanuel.cliente@cliente.com
Hola José Manuel,
Adjunto factura correspondiente al último pedido de mercancía. Te aviso que hemos cambiado de banco. Envío el pedido en cuanto hagas el ingreso.
Saludos,
Factura001_Proveedor.pdf
Enrique Rique
Proveedor S.A.
(+34) 678 910 111

En el correo no había nada fuera de lo normal. Incluso el presunto proveedor, es decir, el falso Enrique, se permitía realizar algunas bromas y se despedía en tono cordial. De modo que José Manuel realizó las transferencias siguiendo las instrucciones y siguió con sus tareas del día a día. Tan solo semanas después, cuando su jefe le advirtió que el pedido de maquinaria no llegaba y, tras ponerse en contacto con el proveedor auténtico y constatar que éste no se había comunicado con ellos, ambos se detuvieron a examinar con más cuidado el correo electrónico que habían recibido.

Lo peor fue descubrir la simpleza del fraude. Al hacker le había bastado con cambiar una letra del dominio del correo para suplantar la identidad del proveedor. Algo que cualquier persona, en el día a día de un trabajo de oficina, puede pasar por alto. ¿El resultado? Una pérdida económica irrecuperable, cancelación de toda la operativa administrativa ("¿Estáis seguros de que éste es el único correo fraudulento que hemos recibido?") y un parón indefinido en la actividad de la empresa.

¿Qué conclusión podemos extraer de esta incidente? Principalmente, que las pequeñas y medianas empresas son especialmente vulnerables a los ciberataques 🔗, con pérdidas que pueden alcanzar los 50.000 euros de media. En 2024, España registró 58 ataques de ransomware solo en el primer semestre, colocándola entre los países más afectados a nivel global. Además, el 96% de las empresas españolas ha sido blanco de ciberataques en el último año, 🔗 con un 66% reportando un aumento en la frecuencia de estos incidentes.



Sobre phishing. Los ataques por medio de phishing son una amenaza constante y creciente para todo tipo de PYMEs.

Algunas de las razones que explican la especial vulnerabilidad de las PYMEs respecto a las amenazas digitales son las siguientes:

- **Recursos limitados en ciberseguridad:** A menudo, las PYMEs carecen de los presupuestos necesarios para implementar medidas de seguridad avanzadas, lo que las deja expuestas a amenazas.

- **Falta de personal especializado:** Muchas pequeñas empresas no cuentan con expertos en ciberseguridad que puedan identificar y mitigar riesgos de manera efectiva.

- **Conciencia limitada sobre amenazas digitales:** La falta de formación en ciberseguridad entre los empleados puede llevar a errores humanos, como caer en trampas de phishing o manipulación social.

- **Infraestructuras tecnológicas obsoletas:** El uso de sistemas y software desactualizados puede presentar vulnerabilidades que los atacantes explotan fácilmente.

- **Percepción errónea de ser un objetivo menor:** Algunas PYMEs creen que, por su tamaño, no serán blanco de ataques, lo que las lleva a descuidar medidas de protección esenciales.

Ok, tu startup to the moon, pero no olvides protegerte: Principales amenazas digitales

Situémonos ahora mentalmente en el típico ambiente startapero. Negocios full digital, gente corriendo de un lado a otro por los pasillos de un coworking, miles de datos en la nube, procesos en los que se prioriza la rapidez antes que la seguridad (“Te mando la base de datos por WhatsApp, ¿vale?”) y un cesto con fruta fresca en el que, por desgracia, alguien se ha comido siempre el último plátano.

Y es que a todos nos encantan las startups. Sobre todo por su espíritu: crecer cuanto más rápido mejor. Al fin y al cabo, la supervivencia de una idea genial depende de la rapidez con la que, en ocasiones, equipos muy reducidos puedan hacerla realidad.

Pero es precisamente este foco en el crecimiento lo que las vuelve vulnerables antes todo tipo de amenazas digitales. Gonzalo Luján, CEO de la startup murciana SECIFY, enfatiza la importancia de la ciberseguridad para las pequeñas y medianas empresas:

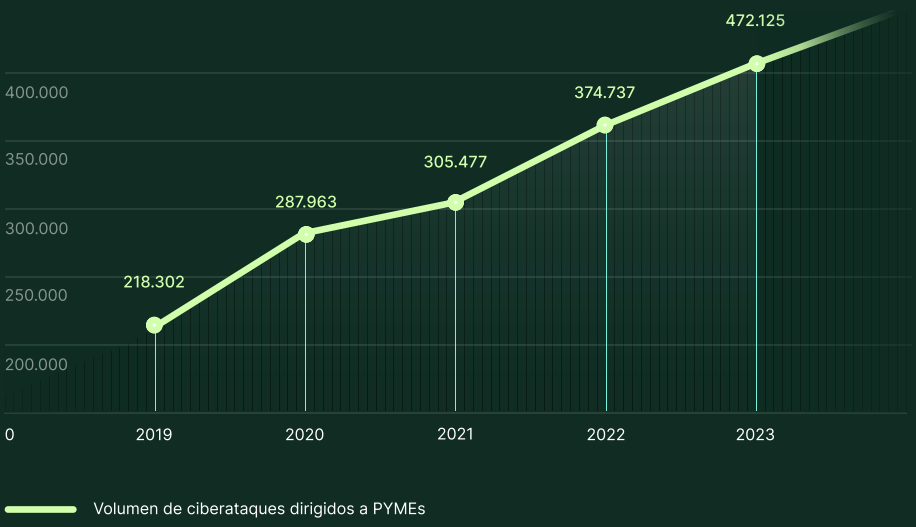
> “Más del 80% de las startups están expuestas a ciberataques, lo que resalta la necesidad de soluciones adaptadas a sus necesidades.”

Un caso bastante sonado que pone de relieve la vulnerabilidad digital de las startups es el sufrido por Dropbox en 2012. Los ciberdelincuentes accedieron a una cuenta de empleado, obteniendo direcciones de correo electrónico de usuarios, lo que resultó en una ola de spam dirigida a estos.

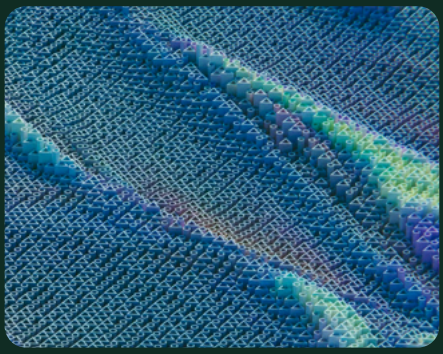
Otro caso, esta vez más reciente, tuvo lugar en 2024. Piratas informáticos tomaron el control de 33 extensiones de Google Chrome, comprometiendo datos de millones de usuarios a nivel mundial. La brecha de seguridad se originó cuando un desarrollador de la startup Cyberhaven fue víctima de un ataque de phishing, lo que permitió a los atacantes acceder y modificar las extensiones. Entre las afectadas se encontraban herramientas de inteligencia artificial y VPNs como VPNCity, Parrot Talks y Uvoice.

Seguir leyendo >>

Ciberataques en PYMEs: Un riesgo creciente en el mundo digital



Fuente: Sistema estadístico de criminalidad



Sobre los avances con IA. Los nuevos desarrollos como la IA traerán consigo nuevas amenazas que tu empresa debe conocer y ser capaz de gestionar.

Freelancers y profesionales independientes: Cuando la responsabilidad es solo tuya

En España, el número de trabajadores autónomos ha experimentado un crecimiento constante. Según datos del Ministerio de Trabajo, en octubre de 2023 se registraron 3.344.771 autónomos, lo que representa un incremento del 0,38% respecto al mismo mes del año anterior.

Si algo caracteriza a los autónomos y freelancers es que, para lo bueno y para lo malo, ellos son los únicos responsables de su trabajo. Y en este punto es necesario precisar qué significa "trabajo" para un autónomo: no es solo su actividad profesional, sino también, en muchos casos, la contabilidad, el marketing, decenas de gestiones administrativas, el soporte al cliente y hasta arreglar un enchufe en el despacho si no hay nadie más que pueda hacerlo.

Para un profesional que ya equilibra múltiples responsabilidades resulta prácticamente imposible dedicar el tiempo y los recursos necesarios para enfrentar eficazmente los crecientes ciberriesgos. En el caso de los freelancers y profesionales independientes, los principales son:

- **Acceso frecuente a redes pública:** La necesidad de trabajar desde diversos lugares lleva a conectarse a redes Wi-Fi públicas, que suelen ser menos seguras y más susceptibles a ataques.

- **Recursos limitados:** A menudo, los autónomos carecen de los recursos financieros y técnicos necesarios para implementar medidas de ciberseguridad robustas.

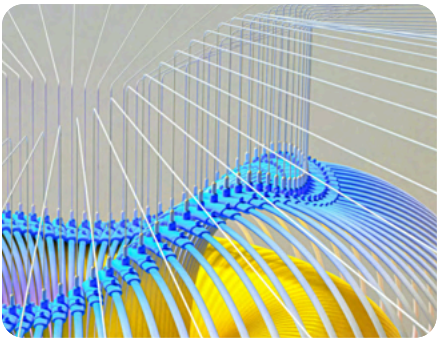
- **Falta de formación especializada:** La ausencia de conocimientos en ciberseguridad puede llevar a prácticas inseguras, como el uso de contraseñas débiles o la falta de actualizaciones en los sistemas.

Axyom quiere plantar cara a las ciberamenazas y estrechar la brecha de acceso a la seguridad digital

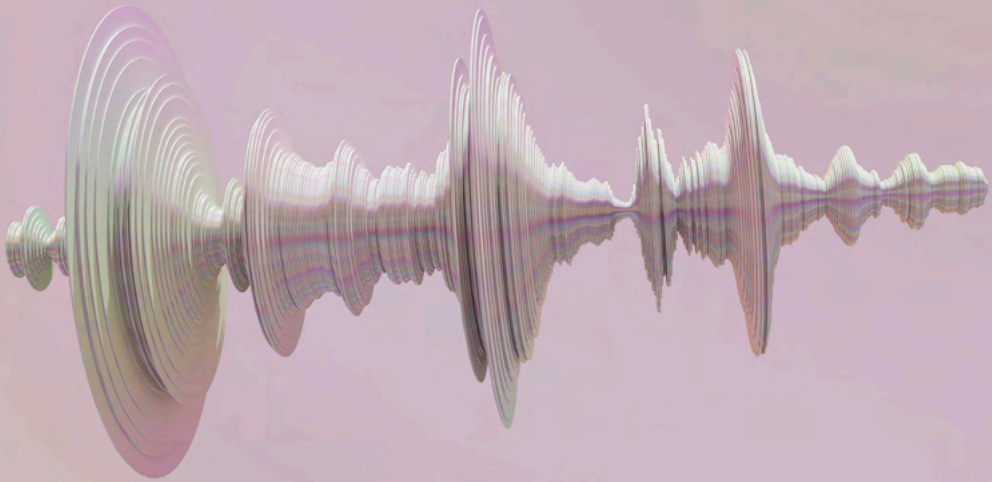
A modo de conclusión, podemos decir que la falta de acceso a soluciones de ciberseguridad adecuadas coloca a las pequeñas empresas y a los freelancers en una posición de gran vulnerabilidad frente a los ciberataques. Sin la infraestructura necesaria para defenderse, cualquier brecha de seguridad puede tener consecuencias devastadoras, desde pérdidas económicas hasta daños irreparables a su reputación.

Pero esto se acabó. Axyom es el primer broker de ciberseguros especializado en PYMEs, startups y profesionales independientes. No solo ponemos a tu alcance soluciones aseguradoras que antes solo estaban reservadas para las grandes corporaciones, sino que además te proporcionamos herramientas proactivas de protección y contenidos especializados para que, a partir de ahora, tus decisiones sobre la ciberseguridad en tu negocio estén basadas en la información más actualizada.

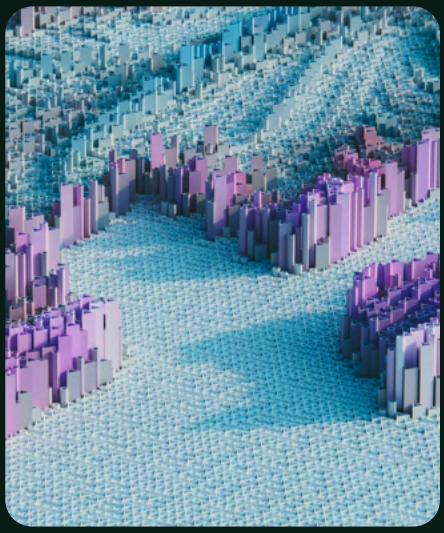
En Axyom, nuestro único empeño es cambiar las reglas del juego para que el tejido de productivo español pueda respirar tranquilo, sentirse protegido ante los riesgos digitales crecientes y dedicarse a lo que mejor sabe hacer: crecer, consolidar su competitividad y hacer realidad las necesidades y sueños de todos sus clientes.



Sobre amenazas digitales. Proteger tu empresa ante amenazas digitales es también cuidar de tus clientes y reputación.



Signals



Sobre ciberataques reales. El conocimiento es poder y redunda en la capacidad de gestión de los ciberriesgos en tu empresa. Cada mes, te presentamos la radiografía de un ciberataque real.

El correo que apagó la empresa: El día que Creativa S.L. cayó en la trampa del ransomware

En la primavera de 2017, una pequeña empresa de diseño gráfico, a la que llamaremos Creativa S.L., operaba en el corazón de Madrid. Con un equipo de diez personas, su reputación se basaba en la entrega puntual y la calidad de sus proyectos. Sin embargo, una serie de acontecimientos inesperados hizo que una mañana a más de uno en la oficina se le atragantara el café del desayuno.

Lunes. 9:30 de la mañana. Laura, responsable de IT de la agencia, enciende su ordenador como de costumbre y de pronto se encuentra con una sorpresa inesperada: todos los archivos habían sido encriptados. Daba igual a cuál intentara acceder. Un mensaje emergente aparecía una y otra vez solicitando un rescate en bitcoins si la empresa quería recuperar los datos.

Sin saberlo, Creativa S.L. había sido víctima del ransomware conocido como WannaCry, un ataque cibernético que, en mayo de 2017, afectó a más de 230,000 computadoras en 150 países. Este malware explotaba una vulnerabilidad en sistemas Windows, encriptando archivos y permitiendo que los ciberdelincuentes amenazaran a las víctimas con hacer públicos los datos si no accedían a sus demandas.

La empresa se enfrentaba ahora a un dilema. Podía pagar el rescate, eso sí, sentando un mal precedente y sin la seguridad de que los ciberdelincuentes exigieran más dinero después. O bien podía negarse, tratar de encontrar el origen de la brecha de seguridad y tratar de mitigar los daños, exponiéndose al daño reputacional que podría ocasionar la publicación de sus archivos.

Seguir leyendo >>

Durante una acalorada reunión, Laura, de pronto, recordó haber recibido varios correos de Microsoft solicitando la descarga de una actualización del sistema operativo. Tras revisar estos correos —casi indistinguibles de los correos oficiales— alguien se dio cuenta de que uno de los archivos correspondientes a la actualización tenía una extensión extraña.

Decididos a no pagar el rescate, el equipo contactó a un experto en ciberseguridad. Este les informó que, aunque existía un parche de seguridad que Microsoft había lanzado en marzo de 2017 para prevenir este tipo de ataques, muchos sistemas, especialmente en pequeñas empresas, no lo habían instalado. Además, les explicó que, aunque algunos investigadores habían encontrado una "vacuna" temporal para detener la propagación del ransomware, no garantizaba la recuperación de los datos ya encriptados.

Con la ayuda del especialista, implementaron medidas para contener la infección y evitar su propagación a otros dispositivos. Sin embargo, la recuperación de los datos resultó ser un proceso complejo. La buena noticia era que contaban con copias de seguridad semanales almacenadas en dispositivos externos, lo que permitió restaurar gran parte de la información, aunque perdieron varios proyectos recientes.

Lamentablemente, el impacto económico en la agencia fue significativo. Pero también comprendieron que, de cara al futuro, debían hacer un esfuerzo por educar a su plantilla en ciberseguridad y contar con las medidas de protección adecuadas ante amenazas digitales.

Levantar una agencia creativa es algo que se hace con años de ilusión y esfuerzo. Ser víctima de un ciberataque, es cuestión de un descuido.

Axyom