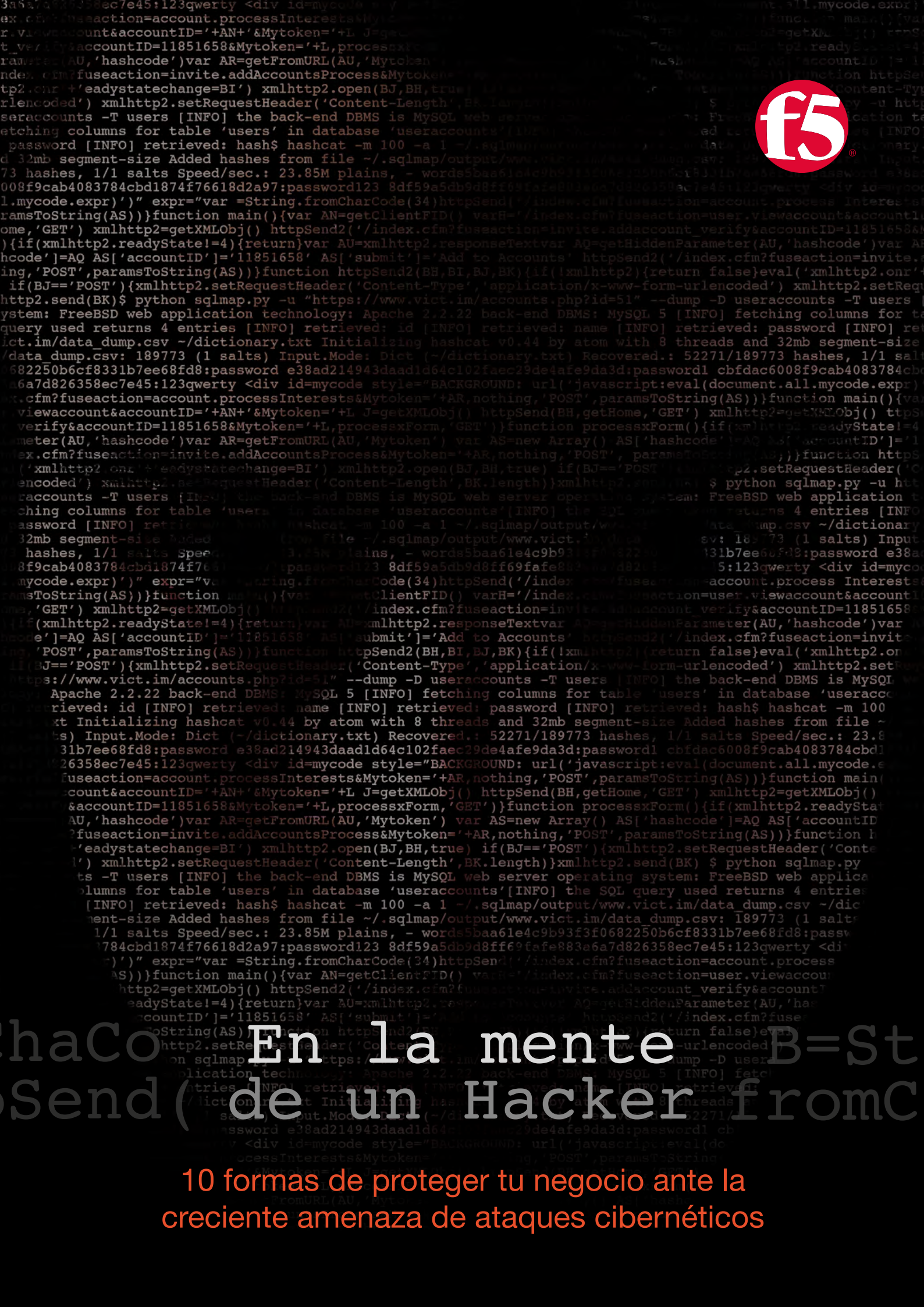
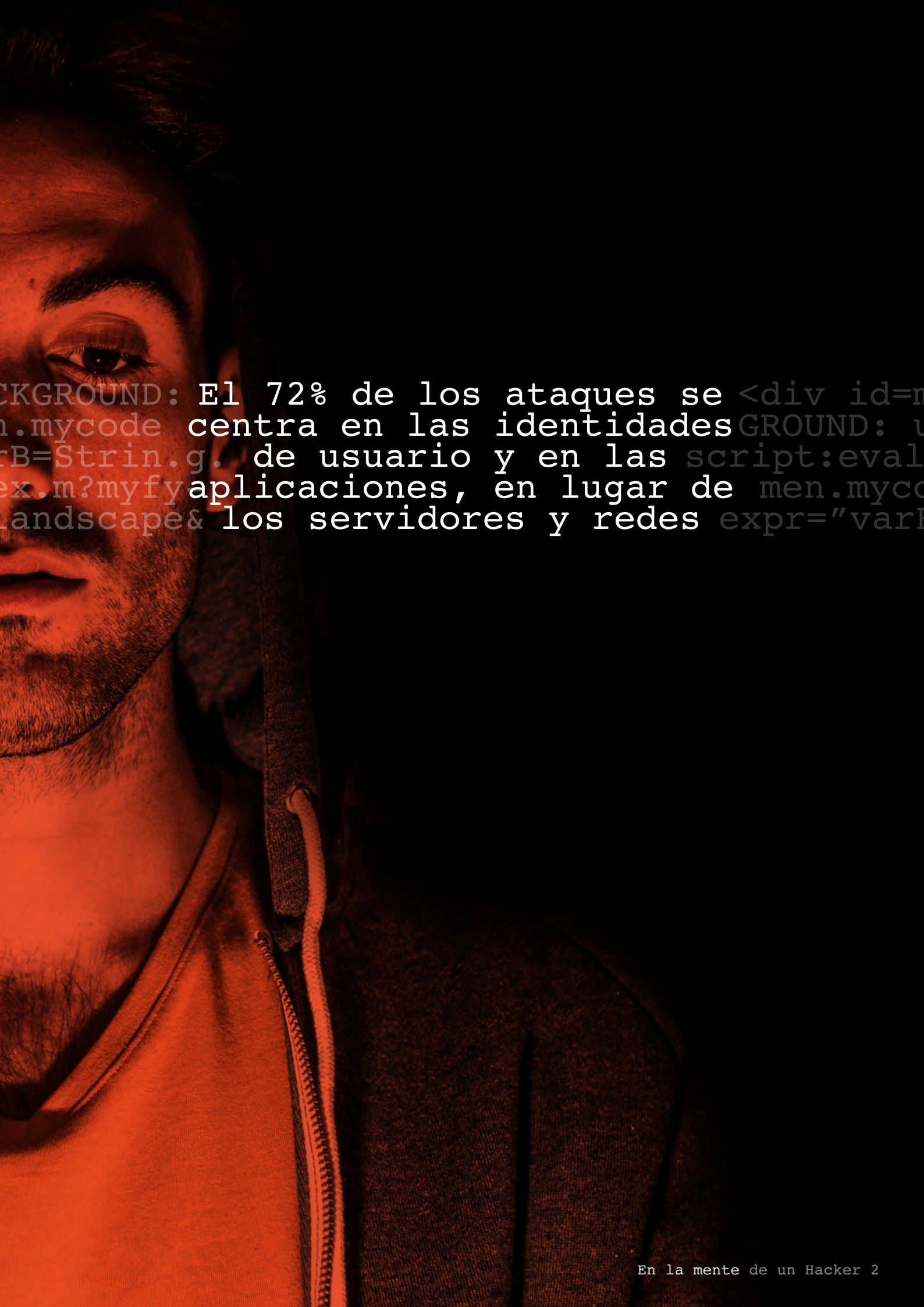


En la mente de un Hacker

10 formas de proteger tu negocio ante la creciente amenaza de ataques cibernéticos


El 72% de los ataques se centra en las identidades de usuario y en las aplicaciones, en lugar de los servidores y redes

En un momento en el que las amenazas cibernéticas están siempre presentes y en constante evolución, la seguridad de la información no es solo un problema informático, sino empresarial. Para las empresas actuales, que basan su negocio en datos accesibles desde cualquier lugar y en cualquier momento, la ruta de acceso ilícita más directa a ellos es mediante aplicaciones que, a menudo, usan identidades de usuario robadas. Por eso no es sorprendente que el 72% de los ataques se centre en las identidades de usuario y en las aplicaciones, en lugar de los servidores y redes. Sin embargo, solo un 10% de los presupuestos de seguridad informática se destina a reducir estas amenazas.

Para que su negocio pueda mantenerse protegido, todos sus profesionales deben comprender las vulnerabilidades, amenazas y riesgos a los que se enfrentan sus operaciones. En esta guía recorremos el panorama actual de seguridad, se analiza por qué, cómo y dónde puede ser vulnerable su negocio, y se ofrecen 12 medidas prácticas que puede adoptar para anticiparse y evitar amenazas inminentes.

La magnitud de la amenaza

La naturaleza, el tipo, el alcance, la frecuencia y la gravedad de los ataques cibernéticos están aumentando extraordinariamente. A diario, se producen casi un millón de amenazas de malware y se hackean cerca de 40 000 webs. En el 2015, 707 millones de registros de datos sufrieron ataques, y se detectaron más de 33 000 webs de suplantación de identidad ('phishing') en una sola semana: un 35% más que el año anterior. Los ataques de denegación de servicio distribuidos (DDoS) [intento de que un servicio en línea quede indisponible sobrecargándolo con tráfico procedente de muchas fuentes], que solían estar únicamente al alcance de hackers experimentados, están creciendo exponencialmente debido, en gran parte, a las herramientas de ataque, fáciles de usar y al alcance de usuarios menos sofisticados y habilidosos.

Existen grupos de hackers que están revisando viejos protocolos que no se habían explotado antes y los ataques de día cero [vulnerabilidad en un código fuente o en un equipo que está siendo utilizado pero que su proveedor o el público desconocen] han sido más del doble en el espacio de un año. Los hackers también actúan a través de las redes sociales, con técnicas como el spear phishing [intento de fraude mediante la falsificación de un mensaje electrónico que se envía a una empresa para acceder a datos confidenciales], o ataques de inyección [mecanismo que combina código malicioso en un programa vulnerable con datos normales que introduce el usuario, a menudo para robar cookies y secuestrar sesiones] donde el contenido generado por el usuario hace que las aplicaciones web se vuelvan vulnerables.

Por muy triste que pueda sonar todo esto, esta es la realidad en la que vivimos. Simple y llanamente: el coste de hacer negocios en un mundo digital.

El perfil del Hacker

Ciberdelincuentes:

es el perfil de hacker más conocido, que pueden ser desde individuos o grupos pequeños hasta grupos delictivos organizados en todo el mundo. Su motivación es bien sencilla: ganar dinero usando cualquier medio disponible, incluido el fraude, el robo de identidad, la suplantación de identidad ('phishing') y los ataques con rescate.

Atacantes financiados por estados:

(estados nación): hacen tareas de ciberespionaje con el fin de robar secretos militares y gubernamentales, así como de propiedad intelectual. Están bien financiados, a menudo por gobiernos, y cuentan con recursos para contratar a los mejores talentos para perpetrar ataques sofisticados, incluidos ataques de día cero (vulnerabilidades previamente desconocidas) y amenazas persistentes avanzadas, que son las que no logran ser detectadas en un sistema o red durante largos periodos de tiempo.

Los hacktivistas:

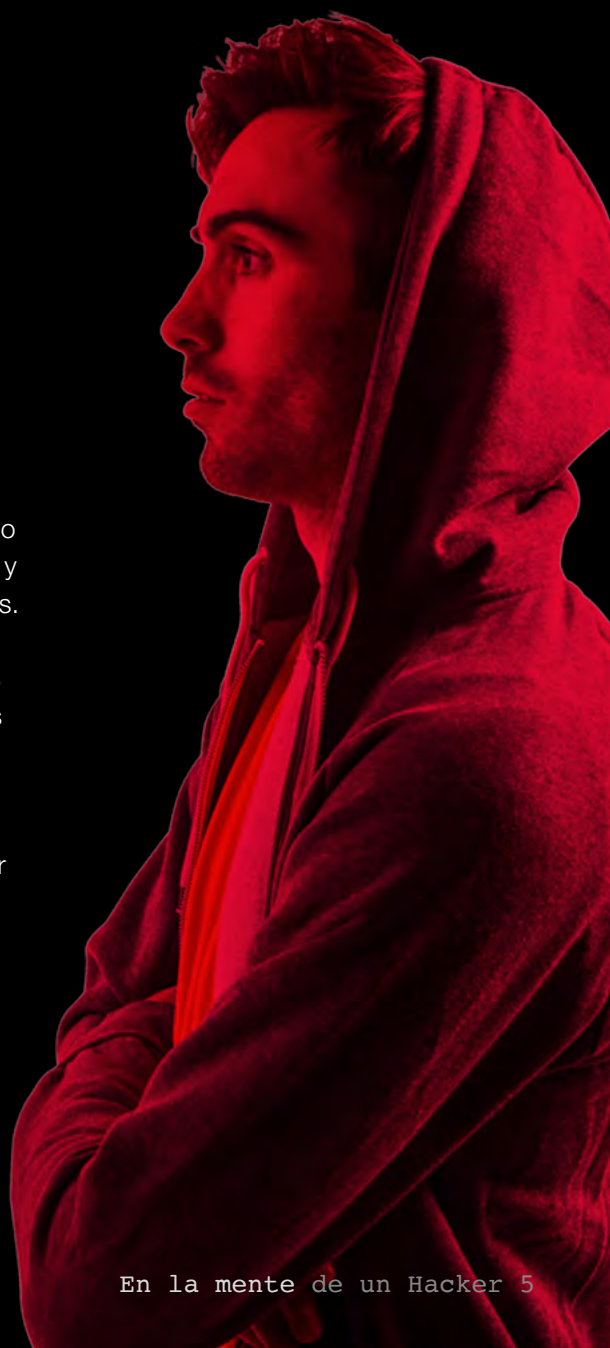
son atacantes con motivaciones políticas y sociales que suelen perpetrar ataques DDoS para derribar sitios web y poner en evidencia a empresas y entidades gubernamentales. Los hacktivistas a menudo no tienen antecedentes penales, pero pueden llegar a estar lo suficientemente motivados emocionalmente como para participar en un delito informático en un intento de hacerse oír. El DDoS, ladeformación de sitios web y las campañas de spam se encuentran entre sus armas más habituales.

Ciberterroristas:

considerados por algunos como el tipo de hacker más peligroso, por tener motivaciones religiosas o políticas. Su objetivo es provocar miedo y caos, conseguir poder y desestabilizar infraestructuras.

Atribución:

Aunque a menudo es difícil atribuir de manera precisa un ataque [descubrimiento de un ataque y asignación de responsabilidad], es frecuente que exista un solapamiento perceptible entre los ciberterroristas y las acciones financiadas por Estados. En muchos casos, es mejor dejar que las agencias legales pertinentes se encarguen de la atribución de los ataques. La empresa, en su lugar, debería centrarse en conocer qué datos pueden considerarse más valiosos para los atacantes y evaluar los diferentes métodos con los que pueden verse comprometidos.



Las nuevas formas de trabajar conllevan nuevas complejidades

Antes, las aplicaciones de empresa solían residir en centros de datos que eran propiedad de aquella, y los usuarios accedían a través de una conexión de red directa. Era relativamente fácil proteger la red y los servidores, con visibilidad y control de ambos, y la seguridad se centraba en fortalecer el perímetro de la red con cortafuegos mayores y mejores, diseñados para mantener alejados a personas con malas intenciones.

Antes, las aplicaciones de empresa solían residir en centros de datos que eran propiedad de aquella, y los usuarios accedían a través de una conexión de red directa. Era relativamente fácil proteger la red y los servidores, con visibilidad y control de ambos, y la seguridad se centraba en fortalecer el perímetro de la red con cortafuegos mayores y mejores, diseñados para mantener alejados a personas con malas intenciones.

Hoy en día, el mundo ha cambiado notablemente. La omnipresencia de internet, la ubicuidad de los dispositivos móviles, el aumento de las redes sociales y los extraordinarios avances en HTML5 y otras tecnologías basadas en web y la nube ha cambiado todo en nuestra manera de vivir, de trabajar y de hacer negocios. El último nivel de complejidad en esta continua evolución es la internet de las cosas (IoT), en donde todos los dispositivos electrónicos imaginables —coches, contadores de agua, semáforos, tostadoras, aviones, marcapasos, incluso la ropa— están conectados a internet.

En el centro de este paisaje cambiante se encuentran las aplicaciones, que utilizamos prácticamente para todo lo que hacemos, y están por todas partes. Casi tres cuartas partes de las empresas han trasladado una parte de sus aplicaciones a nubes públicas o administradas, y han sustituido otras con aplicaciones de «software como un servicio» (SaaS), como Office 365, Google Apps y Salesforce.

Muchas aplicaciones se han convertido en aplicaciones basadas en la web y móviles. Las webs orientadas al público, diseñadas para que acceda cualquier persona, invitan a que entre más gente en la red en lugar de mantenerlos fuera. Como resultado, hay más oportunidades que nunca de que se produzcan ataques cibernéticos.

Estamos cambiando el cuándo, cómo y dónde trabajamos

Las maneras de trabajar están cambiando: cada vez más empleados móviles trabajan desde distintas ubicaciones, a menudo conectados a redes no seguras, como puntos de acceso wifi públicos en cafeterías. Lamentablemente, muchos usuarios no comprenden los riesgos de eludir los controles perimetrales (por ejemplo, conectándose a través de soluciones VPN de terceros), o no comprenden totalmente la importancia de adherirse a las políticas de seguridad. Comparten más información que nunca —a menudo, a través de redes sociales— y mezclan datos personales y de la empresa en diversos dispositivos. Intercambian información confidencial de la empresa con compañeros y colegas a través de memorias USB o aplicaciones como Dropbox, y utilizan contraseñas débiles, viejas o duplicadas en varios sistemas, olvidando a menudo cerrar su sesión.

Lo que es bueno para el usuario puede ser malo para los negocios

Mientras que el avance hacia una internet completamente cifrada, con «SSL en todas partes» pretende mejorar la confidencialida de los individuos —por ejemplo, mediante la protección de las transacciones de banca móvil— al mismo tiempo crea nuevos puntos ciegos para los equipos de TI, ya que las soluciones de seguridad tradicionales (cortafuegos de red, detección de intrusos y protección, y sistemas de prevención de pérdida de datos) no son capaces de descifrar el tráfico cifrado. Los hackers lo saben, lo utilizan en su beneficio y son capaces de sortear las soluciones de inteligencia de red tradicionales que antes los habrían detectado. Incluso las empresas con soluciones avanzadas de seguridad capaces de descifrar el tráfico cifrado desactivan con frecuencia esta función debido al impacto potencial que tiene en el rendimiento.

Todo esto crea un entorno mucho más complejo y vulnerable, donde las aplicaciones pueden estar en cualquier lugar y los datos están en todas partes. Con tantos datos distribuidos por tantos lugares, el perímetro de red tradicional queda disuelto y las empresas tienen ahora menos visibilidad y control que nunca.

Tendencias de seguridad de TI: lo que los estudios nos dicen

Los ataques a nivel de aplicación son peores que los ataques a nivel de red. La capa de aplicación del modelo OSI contiene la interfaz del usuario y otras funciones claves como las interfaces de programación de aplicaciones (APIs), lo que hace que los hackers tengan una mayor superficie de ataque. Cuando se hace uso de esta vulnerabilidad de seguridad, se puede manipular toda la aplicación; se pueden robar los datos de los usuarios o cerrarse la red completamente].

Los encuestados citan la falta de visibilidad a nivel de aplicación como la principal barrera para lograr un planteamiento de seguridad sólido.

63%

de los ataques a nivel de aplicación son más difíciles de detectar que a nivel de red

58%

de los ataques a nivel de aplicación son más graves que a nivel de red

67%

de los ataques a nivel de aplicación son más difíciles de contener que a nivel de red

18%

del gasto en seguridad se asigna a la seguridad de las aplicaciones – menos de la mitad del que se destina a la seguridad de la red

50%

del nivel de aplicación sufre más ataques que el nivel de red

Las aplicaciones móviles y en la nube están proliferando

La informática en la sombra está afectando a la seguridad de las aplicaciones, ya que el crecimiento de las aplicaciones móviles y en la nube se percibe como un aumento significativo de la exposición al riesgo.

1175

cantidad media de aplicaciones en una empresa

31%

de las aplicaciones empresariales se utilizan a través del móvil

33%

de las aplicaciones se consideran fundamentales

66%

de lo equipos de TI no tienen visibilidad de todas las aplicaciones instaladas en su empresa.

37%

de las aplicaciones empresariales están en la nube

El último estudio del Instituto Ponemon, «La seguridad de aplicaciones en el cambiante panorama de riesgos (julio del 2016)», revela algunas inquietantes lagunas en las disposiciones de seguridad según una encuenta hecha en Estados Unidos a los profesionales del sector IT.

No queda claro quién se responsabiliza de la seguridad de las aplicaciones

En la actualidad, la responsabilidad de garantizar la seguridad de las aplicaciones se dispersa en toda la empresa. Con tal fragmentación, no es sorprendente que surjan vulnerabilidades.

56%

creen que la responsabilidad de la seguridad de las aplicaciones está pasando de ser del equipo TI al usuario final o al propietario de la aplicación

20%

piensa las unidades de negocio son las responsables

21%

cree que el responsable es el director de Informática o el director de Tecnología

19%

cree que los equipos de desarrollo de aplicaciones son los responsables

20%

piensa que ninguna persona o departamento es responsable

Las duras consecuencias de un enfoque reactivo

Si no tiene un enfoque proactivo para la seguridad de las aplicaciones, su empresa corre el riesgo de sufrir un incremento en el número de incidentes de seguridad, tanto detectados como no detectados. Puede sufrir pérdidas financieras directas por la fuga de datos, o ver dañada su reputación, lo cual podría disuadir a los inversores y lanzar a los clientes a los brazos de sus competidores. El tiempo y esfuerzo empleados en la investigación de una violación de seguridad después de producirse le distrae de su actividad de negocios principal, y las pérdidas son irrecuperables. Y dado que la seguridad de la información se está convirtiendo en un elemento diferenciador en el mundo conectado actual, puede ver cómo su negocio se queda atrás frente a sus rivales, que pueden ofrecer mayores garantías en cuestiones de privacidad.

10 medidas para fortalecer su planteamiento de seguridad

El motivo de llamar la atención sobre estos riesgos y amenazas no es provocar miedo en las empresas, sino resaltar la proliferación y el impacto de los ataques cibernéticos, y dotar a las empresas con el conocimiento, a través de inteligencia sobre amenazas, para fortalecer su planteamiento de seguridad. A continuación, presentamos una lista de 10 medidas que puede adoptar para tener una estrategia de seguridad y reducción de riesgos sólida y clara.

El 90% de los presupuestos en TI actuales se siguen gastando en todo menos en proteger aplicaciones e identidades de usuario.

1 Crear presupuestos que tengan en cuenta la realidad actual

El 90% de los presupuestos en TI de la actualidad se siguen gastando en todo menos en proteger aplicaciones e identidades de usuario, a pesar de que estos son los principales objetivos de los ataques de hoy en día. Consiga que la junta directiva se involucre preparando a los líderes de la empresa ante la probabilidad y el impacto potencial de un ataque. De esta manera, se asegurará de que las inversiones en seguridad o los programas de formación cuentan con los recursos necesarios y tienen la prioridad adecuada.

2 Conocer los riesgos

F5 puede ayudar a las empresas a obtener la información que necesitan para evaluar riesgos y adoptar las medidas oportunas (véase abajo), pero también es imprescindible que se familiarice con los principales 10 ataques OWASP [Open Web Application Security Project: una organización sin ánimo de lucro especializada en mejorar la seguridad informática]. Este documento informativo describe en detalle las deficiencias de seguridad de las actuales aplicaciones web más críticas y enseña a mitigar determinados tipos de ataques. Las empresas que no siguen estos consejos —y hay muchas— quedan muy expuestas a infracciones de seguridad.

3 Conozca al enemigo

Conozca y comprenda las motivaciones de los hackers, sus objetivos y sus tácticas (véase el perfil del hacker). Los hackers tienen perfiles muy variopintos, pero la mayoría de los que existen en la actualidad son ciberdelincuentes con una sola motivación: el dinero.

Y aunque tienen reputación de perpetrar esquemas sofisticados, la verdad es que muchos de sus métodos no lo son en realidad. En última instancia, se deciden por aquello que menos esfuerzo les suponga —los blancos fáciles— así que es mejor dificultarles la labor.

4 Educar, educar, educar

La seguridad cibernética no es responsabilidad del equipo de TI: es responsabilidad de todos. Las herramientas más sofisticadas de seguridad pueden proteger su negocio frente a una gran cantidad de malware y virus, pero no pueden defender a los usuarios que no practican una 'higiene' cibernética adecuada. Cree una cultura de seguridad en su empresa con la implicación de los altos cargos para que los directivos entiendan de qué manera la seguridad afecta a los resultados y que en última instancia, ellos son responsables del riesgo.

Proporcione a los empleados de todos los niveles las políticas y el conocimiento necesarios para proteger mejor su información mediante un comportamiento proactivo y que tenga en cuenta la seguridad. Haga recordatorios continuos, refuerzos y actualizaciones (la formación no puede ser ocasional) y asegúrese de dar formación adecuada sobre seguridad a los nuevos empleados. Comunique las fugas de datos publicadas, especialmente aquellas provocadas por errores humanos o por medidas de seguridad laxas y cuantifique cómo un incidente similar podría perjudicar a su empresa.

5 Aplicaciones web y dispositivos móviles seguros

Mejore su capacidad para gestionar la vulnerabilidad de las aplicaciones web mediante el uso de un cortafuegos de aplicaciones web (WAF). La codificación segura simplemente no basta para proteger los activos de información. Las vulnerabilidades en lenguajes de desarrollo (por ejemplo, Python), métodos cada vez más complejos de ofuscación, un flujo aparentemente constante de problemas con SSL/TLS, significan que la aplicación de políticas de seguridad para servidores de aplicaciones individuales es imposible o muy difícil a nivel operativo. La seguridad de las aplicaciones requiere una mayor visibilidad mediante la comprensión del contexto de la solicitud, el usuario en cuestión y el dispositivo que utiliza.

Los dispositivos personales están reemplazando rápidamente a los emitidos por las empresas, mucho más controlados. Lleve a cabo una auditoría para asegurarse de que sabe exactamente a qué información se accede en qué dispositivos y si la empresa lo considera un riesgo aceptable. Si no es así, investigue soluciones de espacios aislados[mecanismo de seguridad que permite ejecutar programas o código que no es de confianza sin correr el riesgo de dañar el equipo central o el sistema operativo] y de gestión de identidad y acceso para controlar más estrictamente el acceso a sus datos.

6 Proteger la nube

Si tiene instalado un programa de SaaS o un entorno de alojamiento en la nube, debe exigir a su proveedor al menos las mismas normas que aplicaría a su propio centro de datos, y asegurarse de que no se pueden filtrar los datos de la empresa, que los datos se mantienen en la más estricta confidencialidad y que los puntos de conexión a la red están protegidos. Trasladarse a la nube alivia la carga de poseer y gestionar una infraestructura. Por desgracia, no evita la necesidad de proteger la información. En última instancia, la empresa siempre es la responsable de los riesgos, así que es importante regular las políticas de seguridad, con independencia de dónde residan las aplicaciones y los datos.

7 Sacar al equipo de TI de la sombra

La demanda de nuevas aplicaciones a menudo supera la capacidad del equipo de TI, así que si no puede suministrar los servicios a la velocidad que su empresa exige, las líneas de negocios omitirán al equipo de TI y optarán por infraestructuras y servicios de terceros. Para asegurarse de que un equipo de TI en la sombra no deje expuestos innecesariamente sus datos de empresa o los de sus clientes a riesgos de seguridad y cumplimiento normativo, necesita las herramientas y la visibilidad para suministrar y gestionar su cartera de SaaS de la misma manera que lo haría su propio centro de datos. Operar un modelo de intermediación, con el apoyo de un marco de cumplimiento y de gobernabilidad, y una lista de proveedores aprobados, ayudará a mantener un nivel básico de fiabilidad, disponibilidad y seguridad de los servicios de nube adquiridos por la empresa.

8 Simplificar y reforzar el control del acceso

Los hackers tienen seis veces más éxito en ataques de fuerza bruta, gracias a fallos de seguridad tales como el robo y posterior exposición pública de contraseñas de LinkedIn. Haga todo lo posible para permitir el inicio de sesión único con el fin de reducir el número de contraseñas que se almacenan de forma insegura o que se repiten a través de muchos sistemas críticos, y aplique la autenticación en dos pasos para el acceso a su red y aplicaciones.

9 Escanear, probar y escanear de nuevo

Las vulnerabilidades no son nunca una cuestión eventual; debe tener un proceso de prueba continua con un conjunto completo de herramientas específicas para los sistemas y el software de su entorno. Las pruebas de penetración externa e interna de sus redes, las pruebas de código estático, y las pruebas de caja negra de sus aplicaciones son vitales. Y debe volver a probar las aplicaciones cada vez que haya cambios en el código.

10 Contratar a desarrolladores de aplicaciones expertos en seguridad

Aquellos que entienden y aplican un diseño de aplicaciones seguro, así como prácticas de codificación y prueba pueden reducir sustancialmente los riesgos de seguridad de aplicaciones mediante el uso de técnicas como el modelado de amenazas y el análisis de riesgos de arquitectura. Es especialmente importante realizar pruebas previas en la fase de diseño y desarrollo, en lugar de hacerlo en las fases de lanzamiento y post-lanzamiento, para evitar sorpresas costosas.

10 medidas para **fortalecer** su planteamiento de seguridad

Prácticas recomendadas para usuarios finales

Utilice contraseñas fuertes y únicas para cada cuenta. Utilice un gestor de contraseñas para guardarlas de forma segura.

No utilice nunca redes WiFi abiertas sin establecer automáticamente una conexión VPN segura.

Mantenga el software del sistema operativo actualizado.

Actualice el software anti-virus, anti-malware, anti-spyware y el firewall con regularidad, ya que incluso ellos pueden ser convertirse en vectores para ataques a sus sistemas. Aprenda a diferenciar entre los mensajes del antivirus que son legítimos y los falsos.

Navegue y utilice el correo electrónico con sentido común. Nunca haga clic en enlaces o archivos adjuntos de fuentes desconocidas o poco fiables. Verifique las direcciones web sospechosas antes de hacer clic en ellas.

Resístase a «comodidades» como el uso de sus datos de Facebook para iniciar sesión en otros sitios web o a memorizar contraseñas en las páginas de inicio de sesión web.

No comparta nunca información de la empresa utilizando aplicaciones no autorizadas (como Dropbox).

Comprender las alertas de certificado SSL/TLS del navegador web y entender los riesgos que conlleva – una alerta de certificado podría significar que sus comunicaciones están siendo interceptadas.

La «Información sobre amenazas» de F5 Labs puede ayudar

Hoy en día, pocas empresas cuentan con los recursos internos y la información sobre amenazas necesarios para luchar contra los riesgos cibernéticos sin ayuda de nadie. Aquí es donde F5 Labs entra en juego. Durante más de dos décadas, nos hemos centrado únicamente en el suministro de aplicaciones y seguridad. Tenemos el conocimiento más profundo sobre las aplicaciones y la red, y nuestra ubicación en la red nos proporciona un punto de vista único en el mundo de la seguridad informática.

F5 Labs – nuestro equipo de investigación e inteligencia sobre amenazas – ofrece a la comunidad de seguridad inteligencia sobre amenazas muy útil en relación a las tendencias cibernéticas actuales y futuras para que así puedan mantenerse a la vanguardia de la seguridad. Combinamos la experiencia de nuestros investigadores expertos en seguridad con la magnitud de los datos que recopilamos sobre amenazas de múltiples fuentes, incluida nuestra base de clientes global. Lo examinamos todo, desde los agentes de las amenazas, la naturaleza y el origen de los ataques hasta la evolución de las técnicas, herramientas y tácticas; y generamos análisis de los incidentes significativos después del ataque.

Nuestro objetivo es obtener una visión completa del ámbito de ataque, del mismo modo que lo sufren los clientes. Desde las variantes más novedosas de malware hasta las tendencias y ataques de día cero, en nuestra próxima serie de informes de «Información sobre amenazas» se detallarán los últimos avances del equipo F5 de investigación e información práctica sobre amenazas.

f5.com/labs