Mr.LOOQUER

Estado de ciberseguridad de organizaciones españolas

DICIEMBRE 2019

CONTACT

hi@mrlooquer.com

@mrlooquer

ÍNDICE

Resumen Ejecutivo

El estudio aquí presentado pretende abarcar un segmento de la seguridad informática relacionado con el análisis continuo de seguridad de activos expuestos a internet y ampliarlo a un número significativo de organizaciones desde un punto de vista estadístico con el fin de ofrecer una aproximación sobre el estado de seguridad de las entidades bajo estudio. Se han analizado alrededor de **500 organizaciones de 10 sectores distintos**.

En análisis realizado sobre las organizaciones bajo estudio se realiza en dos fases principales:

- *Descubrimiento de activos de la organización. Un activo expuesto es considerado en este estudio un dominio, una dirección IPv4 o IPv6.*
- *Análisis de seguridad de los activos atribuidos a la organización.*

El procedimiento para el descubrimiento y atribución de activos a las organizaciones se detalla en la sección "*Metodología del estudio*" de este mismo documento, al igual que el análisis de seguridad.

Distribución geográfica de los activos analizados en el estudio.

Principales conclusiones

Los 10 sectores analizados presentan un estado seguridad variable en términos cuantitativos, siendo significativa la diferencia en algunos casos. Sin embargo, no se ha detectado que exista una correlación directa entre criticidad de la información manejada o dependencia tecnológica como base del modelo de negocio y el nivel de seguridad.

En cuanto al **perímetro de activos expuestos a internet**, los sectores que presentan un mayor número de activos es el de *Transporte Y Almacenamiento* y *Actividades De Consultoría*, y los que menor superficie de exposición presentan son los de *Suministro De Energía Eléctrica* y *Seguros*, siendo esta diferencia de **hasta 10 veces** superior.

El sector que presenta un menor número de problemas de seguridad es el de **Seguros**, con una disminución significativa en términos cuantitativos en todas las categorías de seguridad analizadas.

En el lado opuesto, los sectores de **Comercio** - tanto al por mayor como al por menor - presentan un mayor número de problemas de seguridad.

Un alto porcentaje de organizaciones presentan problemas de seguridad que pudieran suponer un **potencial incumplimiento de GDPR** desde el punto de vista de asegurar el principio de integridad y protección para el manejo de datos personales de los usuarios. Esto es indicativo del trabajo pendiente de abordar en términos técnicos para mejorar esta parte del cumplimiento.

Es destacable la **alta frecuencia** con la que se encuentran problemas de seguridad de tipo **puertos inseguros expuestos** y **configuración de correo electrónico inseguro**. El impacto de sufrir ataques aprovechando estas debilidades es de sobra conocido, como ataques sobre bases de datos expuestas o suplantación de identidad, sin embargo, en ambos casos, los fallos de seguridad no suelen se complejos de corregir y pasan por añadir una regla de filtrado en un firewall o cambiar opciones de configuración en los servidores de correo electrónico.

Otros datos remarcables resultado de analizar la relación de entidades afectadas por vulnerabilidades más destacables son:

- El **52,94 %** de organizaciones presentan problemas de seguridad relacionadas con el estándar DMARC (Autenticación de mensajes, informes y conformidad basada en dominios). El sector más afectado por este tipo de problemas es *Transporte y Almacenamiento*.
- El **44,78 %** de las compañías tienen Bases de Datos expuestas a Internet.
- El **15,37 %** de las compañías exponen en Internet servicios que pueden llegar a considerarse potencialmente inseguros como SMB (Server Message Block) o NFS (Network File System).
- El **25,61 %** de las compañías presentan algoritmos inseguros SSL (Secure Sockets Layer) y/o certificados autofirmados .
- El **28,75 %** de las compañías tienen issues relacionados con CMS (Content Management System).
- El **76,09 %** de las compañías presentan potenciales incumplimientos GDPR (General Data Protection Regulation).
- El **61,29 %** de las compañías tienen software vulnerable expuesto a Internet.
- El **41,36 %** de los puertos SSH (Secure Shell) accesibles.
- Tan solo un **14,47 %** de compañías usan correctamente cabeceras HTTP para la protección contra ataques de inyección XSS.

Resultados destacables

Vivimos en una época compleja para el mundo de la seguridad informática. Durante años ha estado cambiando el entorno tecnológico en el que las organizaciones se mueven. Por un lado, son enormes las oportunidades que la digitalización ha ofrecido al crecimiento de las empresas, pero por otro, el viaje hacia una evolución constante de los elementos tecnológicos ha dificultado en muchos casos una evolución adecuada también en términos de seguridad.

Es de vital importancia que las empresas y organizaciones conozcan los riesgos a los que se exponen y poder analizarlos de forma precisa de cara a tener el mejor contexto posible para contar con un entorno adecuado en la toma de decisiones.

Este documento es el primero de una serie de publicaciones que ahondarán más en detalles sobre diversos aspectos, como analizar los resultados de sectores determinados, u organizaciones de un determinado tamaño.

Las comprobaciones de seguridad realizadas han sido efectuadas con fuentes de datos obtenidas por MrLOOQUER Rating mediante una infraestructura propia de sondeo. Los análisis realizados han estado centrados en una serie de comprobaciones que se pueden clasificar en las siguientes categorías:

- Seguridad web
- Puertos inseguros
- Correo electrónico
- Análisis de plugins de gestores de contenidos CMS
- Cifrado inseguro
- Vulnerabilidades conocidas

Los sectores analizados para este estudio han sido:

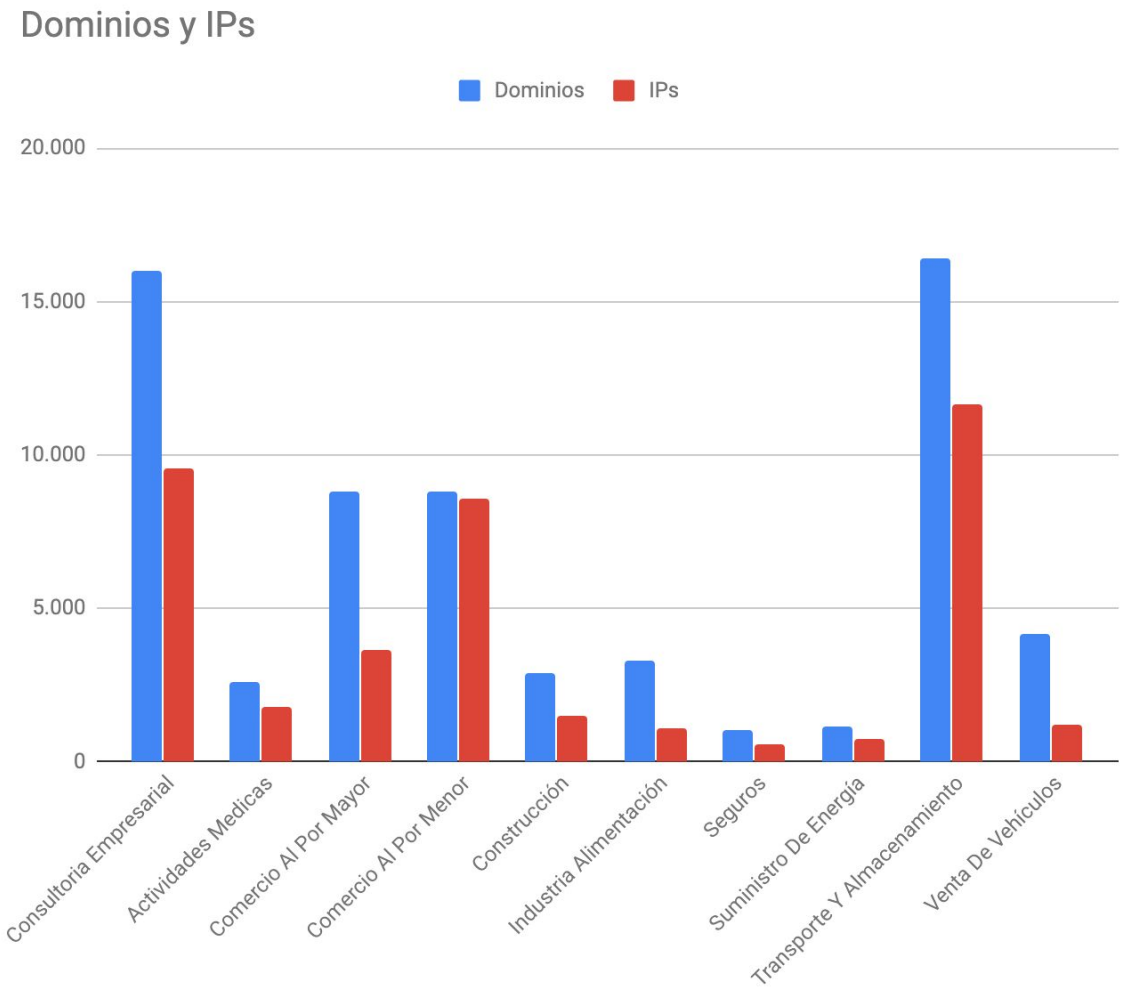
- Transporte Y Almacenamiento
- Actividades De Consultoria De Gestion Empresarial
- Comercio Al Por Mayor E Intermediarios Del Comercio
- Comercio Al Por Menor
- Venta De Vehículos De Motor
- Industria De La Alimentación
- Construcción
- Actividades Medicas Y Odontologicas
- Suministro De Energ Electrica Gas Vapor Y Aire Acondicionado
- Seguros

Distribución de activos por sector

Esta sección pretende dar información sobre la superficie de ataque de las organizaciones dividido por sector. Se pretende así entender qué organizaciones suelen tener mayor número de activos expuestos a internet dependiendo de su actividad. Esta información es clave para este estudio ya que se analizarán el número de debilidades encontradas en relación al número de activos que tenga cada entidad.

En la siguiente gráfica se puede observar un resumen del número de direcciones IP y dominios descubierto en los sectores analizados.

Cabe destacar que sectores como el de la Consultoría o el de Transporte y almacenamiento presentan un número de activos sensiblemente superior al del resto de sectores, siendo el de Seguros y Suministro de Energía de los que menos activos presentan a priori.



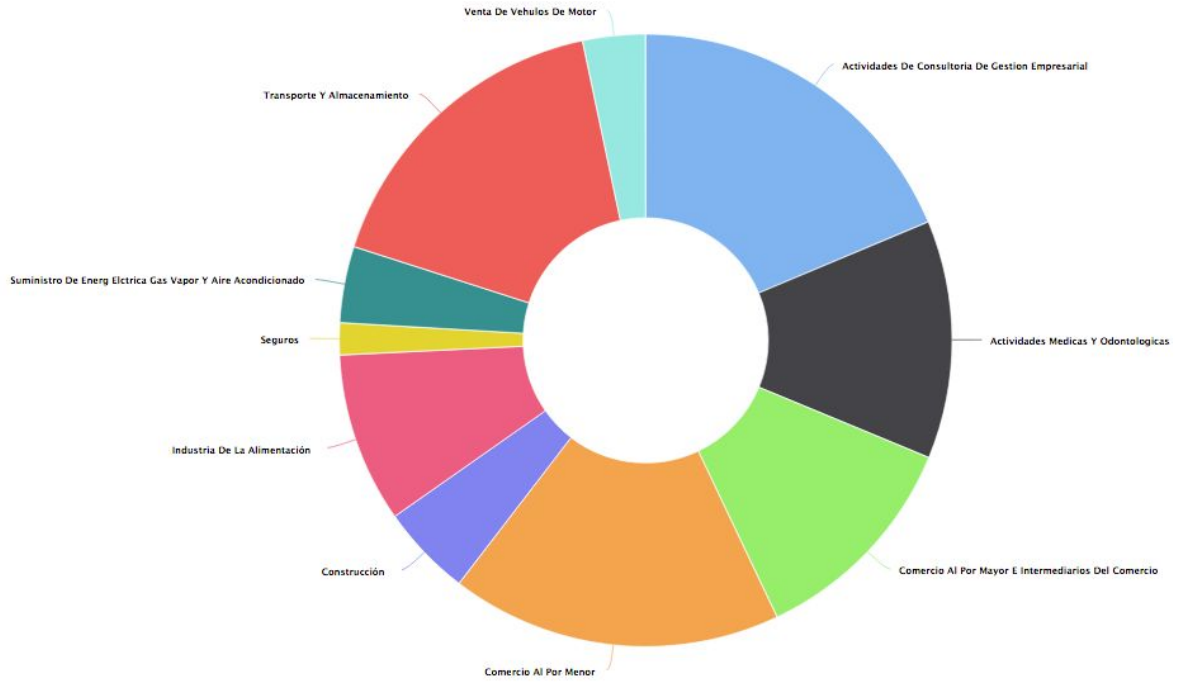
Sin embargo, a pesar de que pudiera parecer que la superficie de ataque es muy variable según organizaciones de distinto sector, como se verá a continuación, la presencia de vulnerabilidades afecta de forma independiente a este factor a los diversos sectores.

Distribución de problemas de seguridad por sector

Al igual que en el apartado anterior estos datos agregados muestran la distribución de las Issues detectadas en cada uno de los sectores analizados.

En la gráfica podemos observar que existen diferencias entre los sectores analizados. **Venta de Vehículos de Motor y Seguros son los menos afectados respecto del resto.**

Por otro lado los más expuestos han resultado ser **Transporte y Almacenamiento, Actividades de Consultoría, Comercio Al por Mayor y al por Menor acaparan casi el 60% de los problemas detectados.**

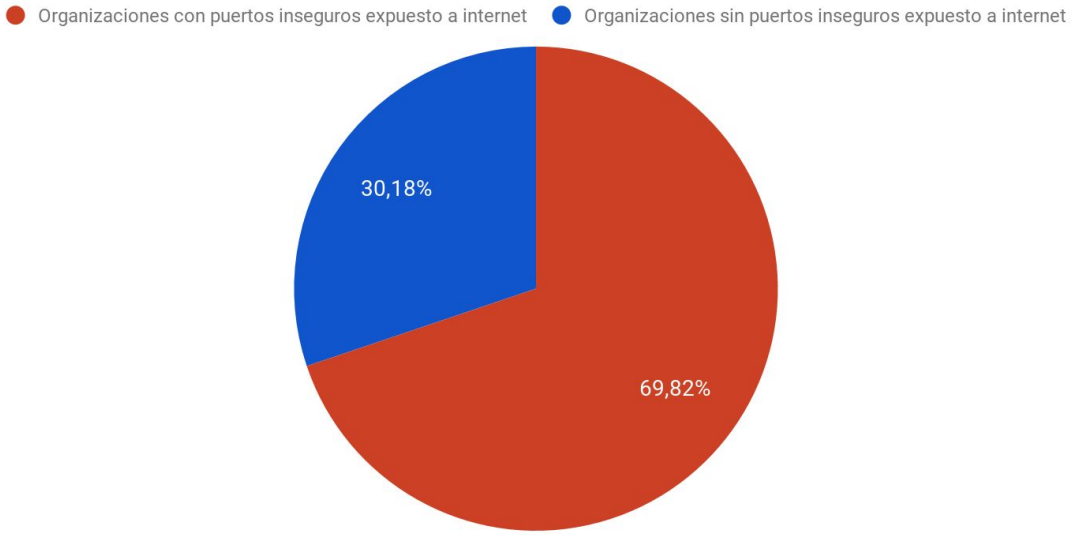


En las siguientes secciones se ofrece información más concreta sobre la presencia y distribución de determinados fallos de seguridad concretos.

Presencia de puertos inseguros abiertos

Se ha detectado que es muy frecuente encontrar organizaciones con puertos inseguros expuestos a internet independientemente del sector. Esta situación es especialmente digna de mención debido al riesgo real que supone para las entidades bajo estudio. El impacto de explotar un puerto inseguro suele ser muy alto, sin embargo, la solución a este tipo de problema suele ser sencilla pasando por configurar de forma correcta las reglas de firewall de entrada de la red de la organización.

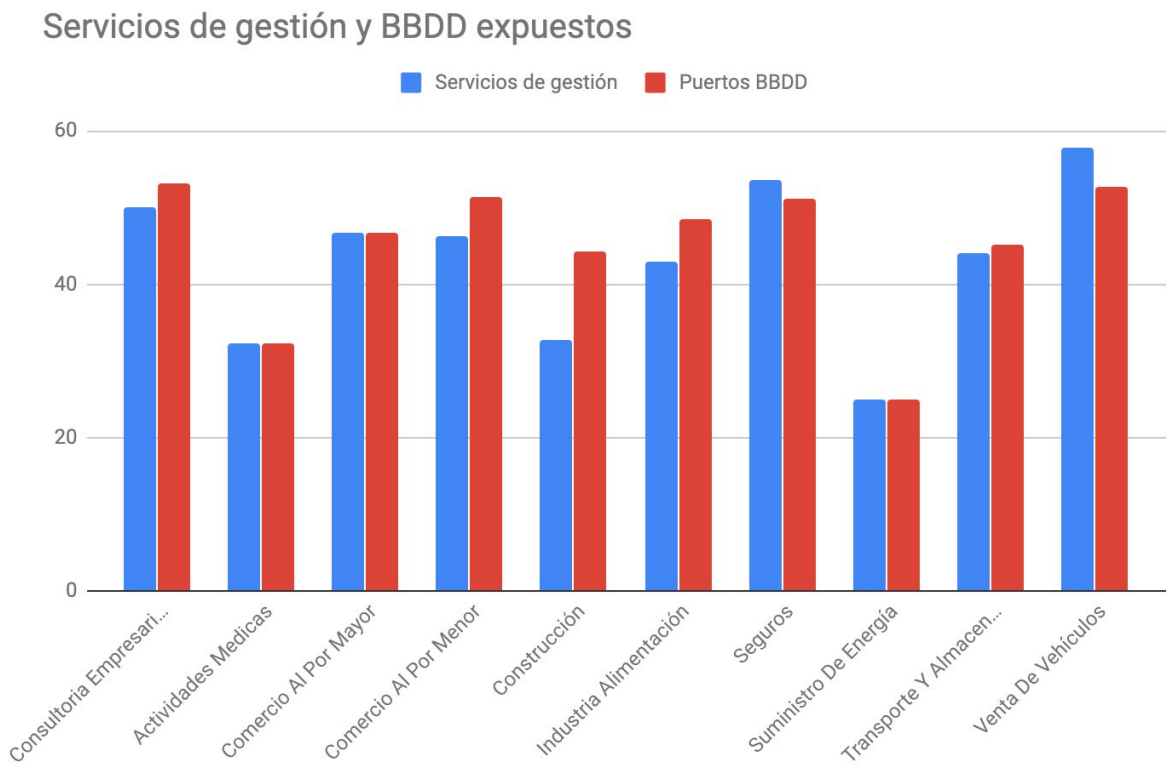
En la siguiente gráfica se puede observar que el **69,82 % de compañías analizadas tenían al menos un puerto inseguro expuesto a internet.**



Estos datos son altamente preocupantes por el riesgo que suponen estas ocurrencias de seguridad para las organizaciones. Si analizamos además la relación con entidades que además exponen servicios de gestión a internet, vemos que ambos datos están altamente relacionados.

Los servicios de gestión como SSH se recomienda que estén expuestos redes protegidas y controladas y que no estén expuestos a internet. Esto se consigue mediante tecnologías como VPN. El que un servicio de gestión esté expuesto a internet hace posible que un atacante realice ataques de diversa índole, como ataques de fuerza bruta, lo cual supone un riesgo innecesario y una práctica mejorable desde el punto vista de seguridad.

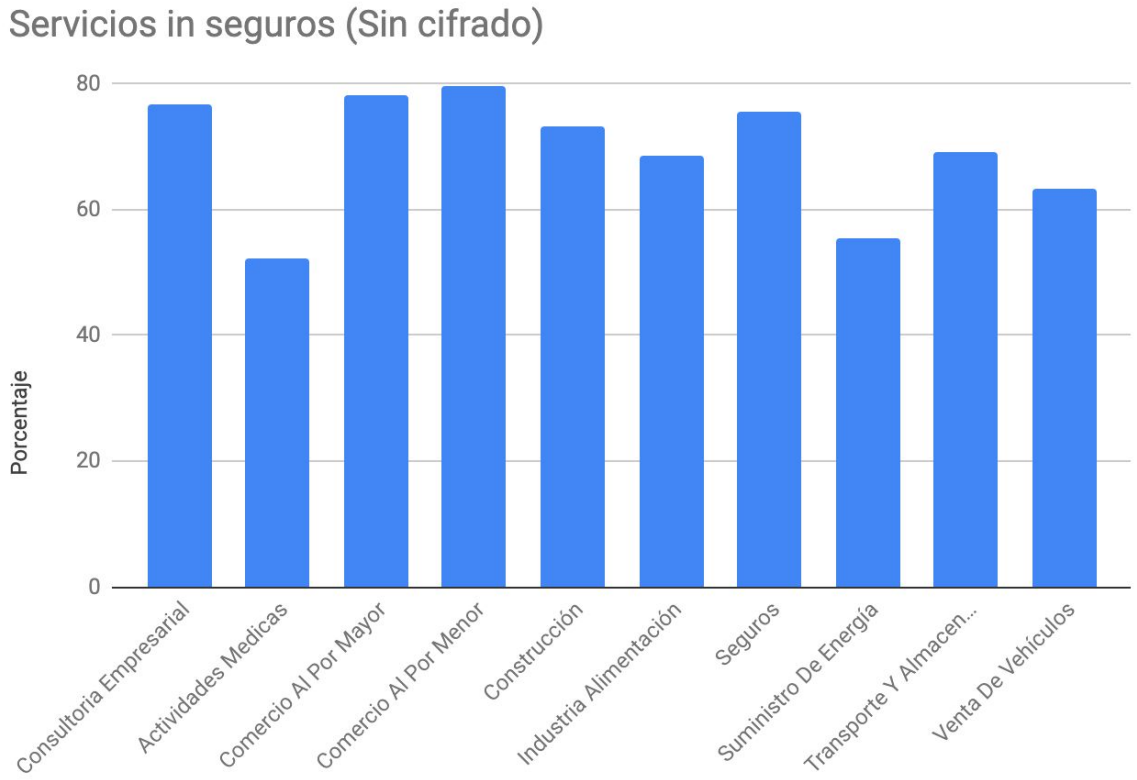
En la siguiente gráfica vemos la relación de compañías con bases de datos expuestas a internet y servicios expuestos a internet.



Por otro lado, es importante asegurar al máximo las comunicaciones con los usuarios usando cifrado del tráfico mediante servicios estándar que usan SSL/TLS. Sin embargo, se siguen usando un número muy elevado de servicios que transmiten la información en claro, por ejemplo FTP (File Transfer Protocol), POP3 (Post Office Protocol) o IMAP2 (Internet Message Access Protocol). Los motivos por los que se siguen usando estos servicios son varios, por ejemplo, por retrocompatibilidad con sistemas legacy. En cualquier caso se presta poca atención al uso de estos servicios y no se le da la importancia que tiene ya que parece, a priori, que el impacto y la probabilidad de ataque no es escalable. Sin embargo, en el lado opuesto está la sencillez de implantar medidas técnicas para no usar este tipo de servicios.

Esta situación conlleva que un atacante pueda conseguir fácilmente acceso a la información intercambiada con los servidores de las entidades si se tiene acceso al tráfico en origen o destino.

A continuación se muestra el gráfico correspondiente con el porcentaje de compañías que siguen usando puertos inseguros sin usar cifrado. Resulta llamativo el alto número de organizaciones que siguen esta práctica, llegando en muchos casos casi al **80% de las entidades del sector**.

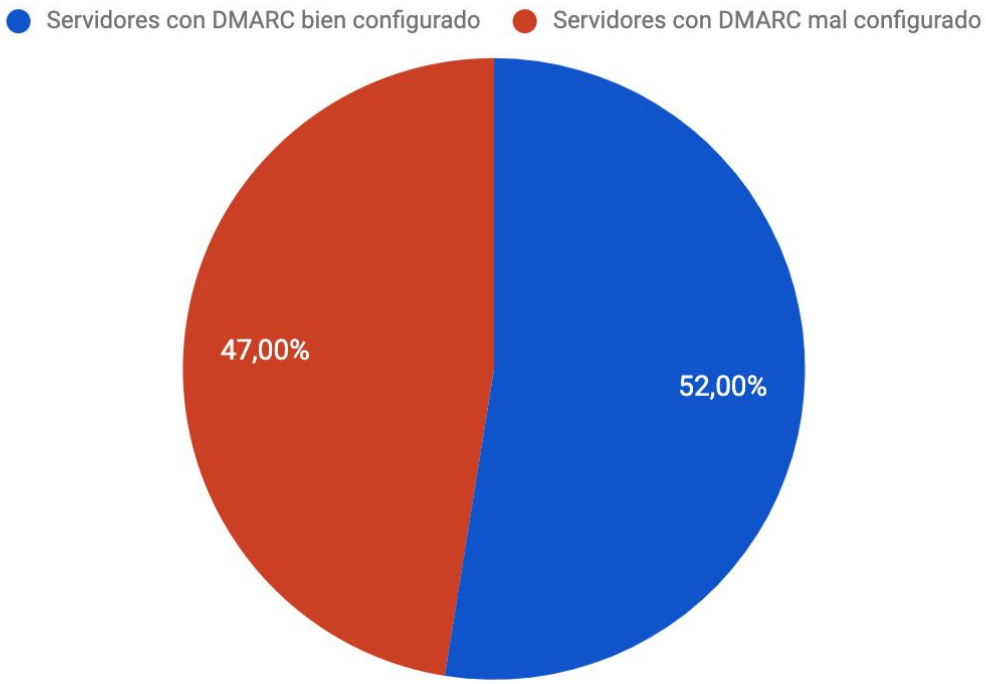


Estado de seguridad de servicios de correo electrónico

Los servidores de correo electrónico ofrecen muchas configuraciones de seguridad que, bien configuradas, permiten a las organizaciones controlar muchos de los ataques que de otra forma se podrían realizar sobre estos servicios, como los de suplantación de identidad o de confidencialidad.

Los servicios de MrLOOQUER analizan diversas configuraciones de los servidores de correo de las entidades para detectar mejoras que puedan aplicarse para mejorar la seguridad.

Se ha tratado de analizar en qué grado se producen incorrectas políticas de seguridad, como ejemplo, a continuación se ofrece un gráfico con el porcentaje total de organizaciones analizadas que presentan servidores con DMARC bien configurados. Resulta preocupante que esta capacidad de seguridad tan recomendable como es **DMARC no la están usando bien un 47% de las organizaciones** analizadas.



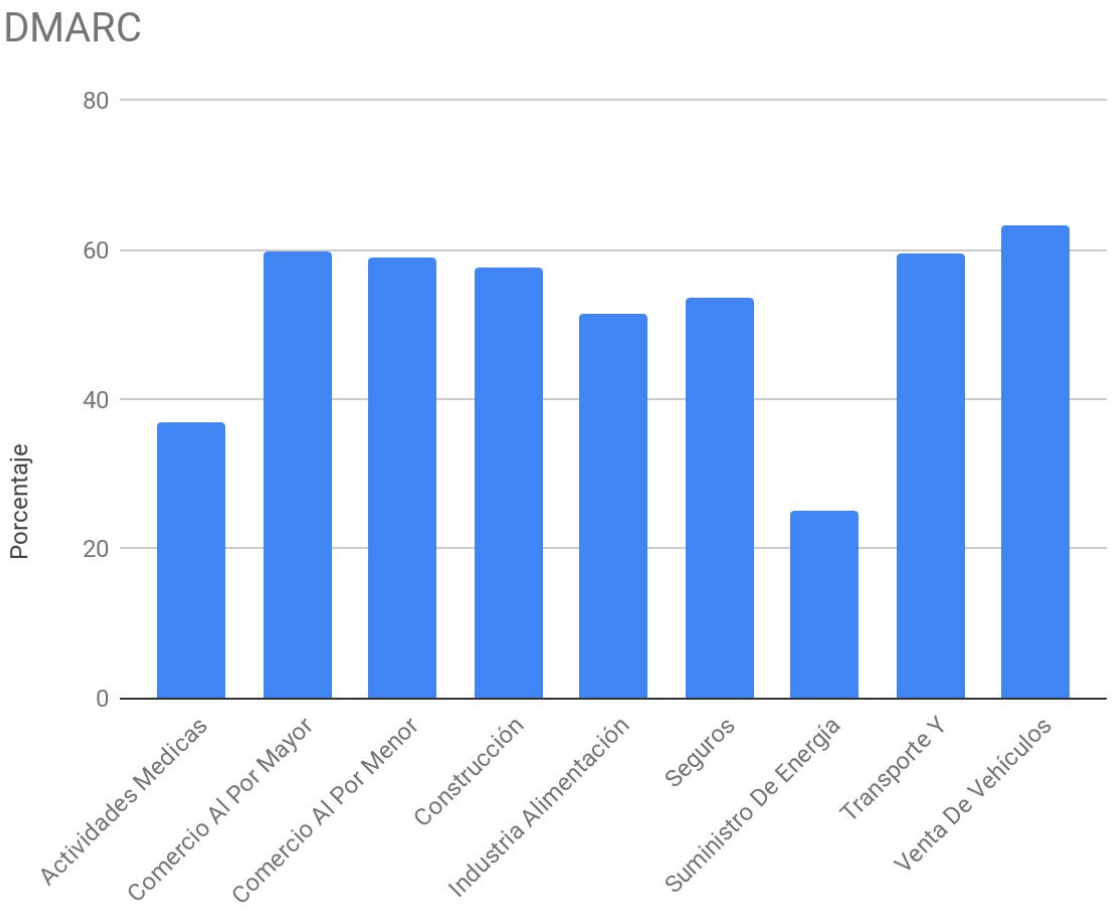
Una organización que no hace buen uso de los protocolos DMARC tiene más probabilidad de sufrir **ataques de phishing y suplantación de identidad.** Este tipo de ataques son usados como punto de entrada para ataques *Ransomware* o de tipo BEC ("compromiso de correos electrónicos corporativos", por sus siglas en inglés). La mayoría de servidores de correo soportan los mecanismos de seguridad DMARC para:

- Que el servidor pueda realizar autenticación de correo electrónico y comprobar que la dirección de correo electrónicos no ha falsificada.
- Aplicar políticas a los mensajes de correo que fallan en la autenticación, por ejemplo "cuarentena" o "rechazar".

A pesar de ser una opción de seguridad disponible para la mayoría de entornos tecnológicos seguimos detectando un alto porcentaje de organizaciones que no terminan de implementar DMARC de forma correcta.

En la siguiente gráfica se puede ver el porcentaje de empresas por sector que presenta algún tipo de problemas de configuración DMARC, superando en muchos casos el 50% de las organizaciones.

La planificación y el despliegue de una configuración DMARC restrictiva adecuada puede llevar tiempo, existiendo tres niveles de política DMARC, sin embargo, esta inversión puede mejorar enormemente el nivel de seguridad de los servidores de correo electrónico interno y externo de una empresa.



Los controles DMARC han estado disponibles durante varios años y son compatibles con prácticamente todos los principales proveedores de correo electrónico. Originalmente implementado como una mitigación contra los ataques de phishing procedentes de agentes externos de una empresa, DMARC también permite que sea mucho más difícil falsificar direcciones de correo electrónico internas.

Gestores de contenido CMS con plugins o temas vulnerables

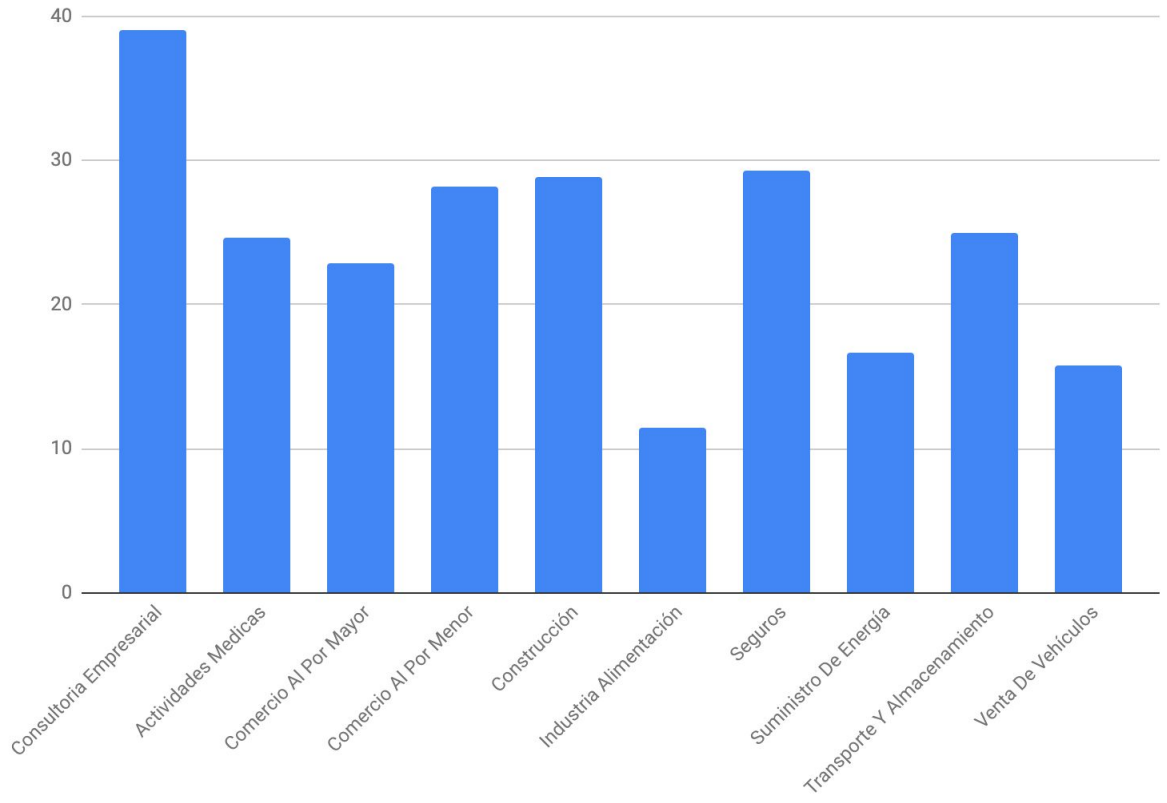
En los análisis llevados a cabo en este estudio se han incluido pruebas en cada de red y en capa de aplicación. Una de las comprobaciones que MrLOOQUER realiza en capa de aplicación es analizar los plugins que usan los CMS detectados en los activos de las organizaciones.

Los gestores de contenidos (CMS), por ejemplo, Wordpres, usan en muchas ocasiones plugins para incrementar la funcionalidad que ofrecen por defecto estas herramienta (Wordpress).

Estos plugins son piezas de software que la mayoría de ocasiones se implementan de forma independiente y que también pueden presentar vulnerabilidades. MrLOOQUER analiza si los plugins instalados en el CMS bajo análisis presenta vulnerabilidades conocidas.

Una vulnerabilidad en un **plugin o un tema de un CMS** puede suponer un riesgo elevado y ser una puerta de entrada para los atacantes. Un atacante podría llegar a hacerse con el control del gestor o llevarse los datos que maneje el site, por ejemplo, datos de usuarios (incluyendo datos personales) y, en este caso, podría suponer una infracción que podría acabar en una sanción por incumplimiento GDPR.

En la siguiente gráfica se puede ver cómo todos los sectores tienen organizaciones que presentan alguna ocurrencia de seguridad relacionada con estos plugins. En el caso del sector **Consultoría casi el 40% de las organizaciones presentan este tipo de problemas**.



También resulta destacable la alta presencia de gestores de contenidos con plugins en todos los sectores analizados.

Configuración de seguridad de servicios de cifrado

El uso de algoritmos y protocolos de cifrado en las comunicaciones en internet resulta de una importancia clave para asegurar la confidencialidad e integridad de las comunicaciones de los usuarios. Existen multitud de complementos para incluir capa de cifrado de las comunicaciones en la mayoría de servicios, y muchos de los productos ya lo ofrecen por defecto.

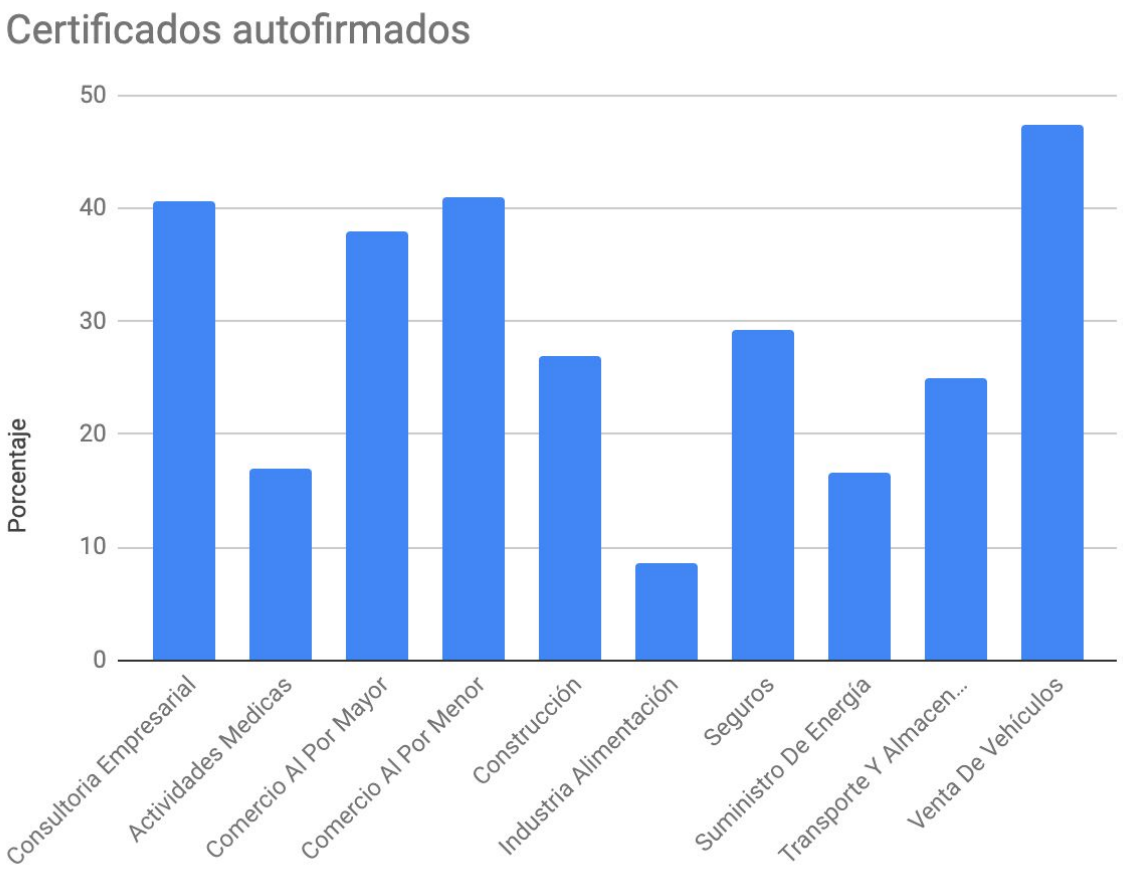
Sin embargo, durante el estudio se ha visto que no solo no se usan mayoritariamente servicios que ofrecen cifrado de las comunicaciones por defecto sino que muchas veces los elementos encargados de asegurar el cifrado no están configurados correctamente.

Se ha detectado una alta presencia de dos principales fallos en la configuración de servicios de cifrado como:

- Certificados autofirmados
- Certificados con algoritmos débiles soportados

En el caso de los certificados autofirmados resulta especialmente llamativo ya que la mayoría de las veces suele ser un fallo asumido al que no se le considera un fallo grave. Los usuarios que visitan estos servicios, por ejemplo, empleados que acceden a alguna web corporativa están acostumbrados a la alerta que los navegadores presentan y no dan importancia al hecho de que la confidencialidad de sus comunicaciones pueden estar siendo comprometidas por cualquier otro elemento que se encuentre en su misma red.

Podemos considerar este fallo de seguridad como **síntoma de una total ausencia de buenas prácticas de seguridad**. El número de ocurrencias de esta vulnerabilidad es tan alto que no hace pensar que pueda ser accidental o puntual, lo cual resulta preocupante. En la siguiente gráfica se puede observar cómo en algunos casos, como en el **sector Venta de Vehículos el porcentaje de empresas con certificados autofirmados casi alcanza el 50%**.



Presencia de vulnerabilidades conocidas

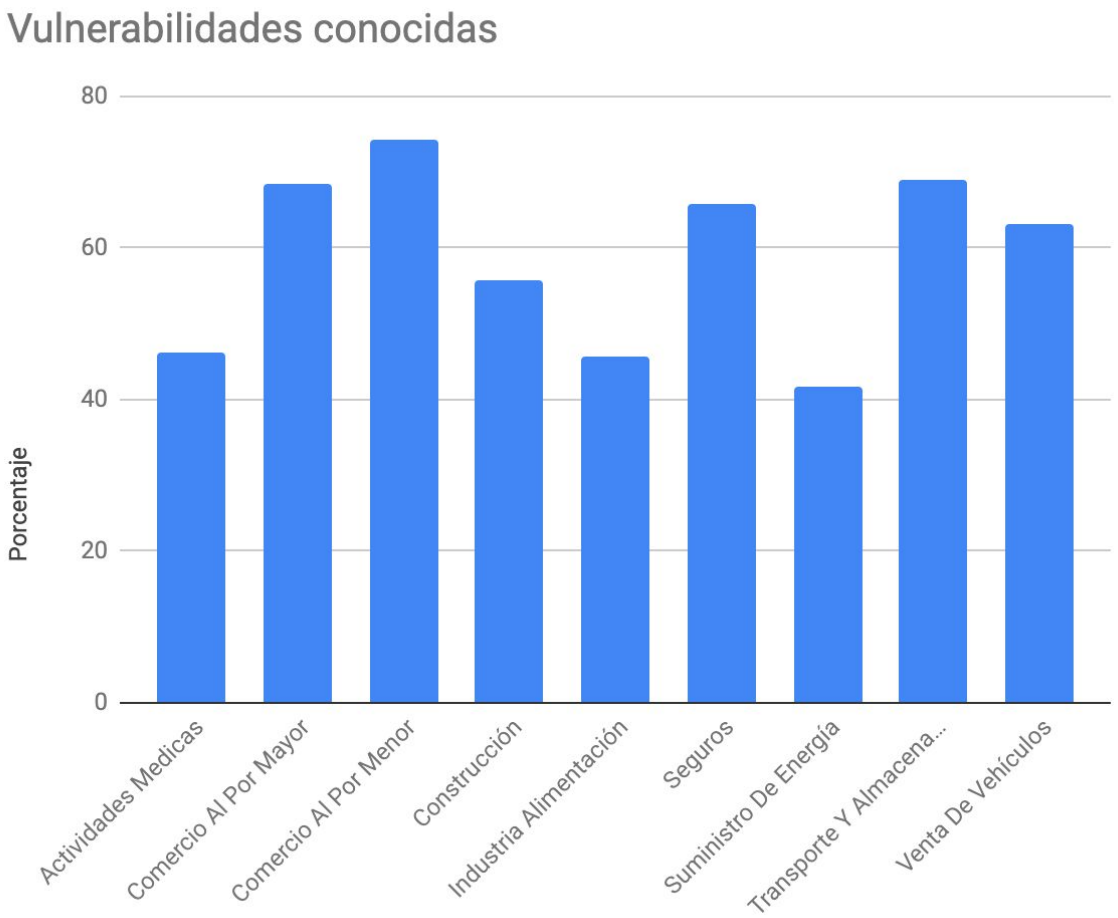
Una correcta política de actualización y parcheo del software que usan las organizaciones es uno de los mayores retos al que se enfrentan los responsables de sistemas y de seguridad. Además, cuanto mayor es la organización, esta tarea puede convertirse en algo inmanejable.

No resulta por tanto de extrañar que se hayan detectado un altísimo porcentaje de organizaciones con servicios expuestos a internet que presentan vulnerabilidades conocidas asociadas.

El proceso de análisis para este tipo de vulnerabilidades es sencillo, primero se detecta la versión del servicio descubierto mediante técnicas de *fingerprinting*. Una vez conocida la versión, solo hay que consultar a una de las múltiples bases de datos de vulnerabilidades conocidas disponibles.

Es importante destacar que el hecho de que se detecten vulnerabilidades asociadas con un identificador CVE (Common Vulnerabilities and Exposures) no implica un riesgo elevado o inmediato, ya que cada vulnerabilidad tiene a su vez una puntuación en base a la criticidad de la vulnerabilidad. En cualquier caso, **siempre es recomendable mantener los servicios actualizados a la última versión en espacio de tiempo razonable**. Más aún cuando se trata de servicios expuestos a internet y que pueden ser atacados desde cualquier punto de internet.

En la siguiente gráfica podemos observar cómo **una media del 50% de entidades** de cada sector **presenta algún servicio con vulnerabilidades conocidas** asociadas.



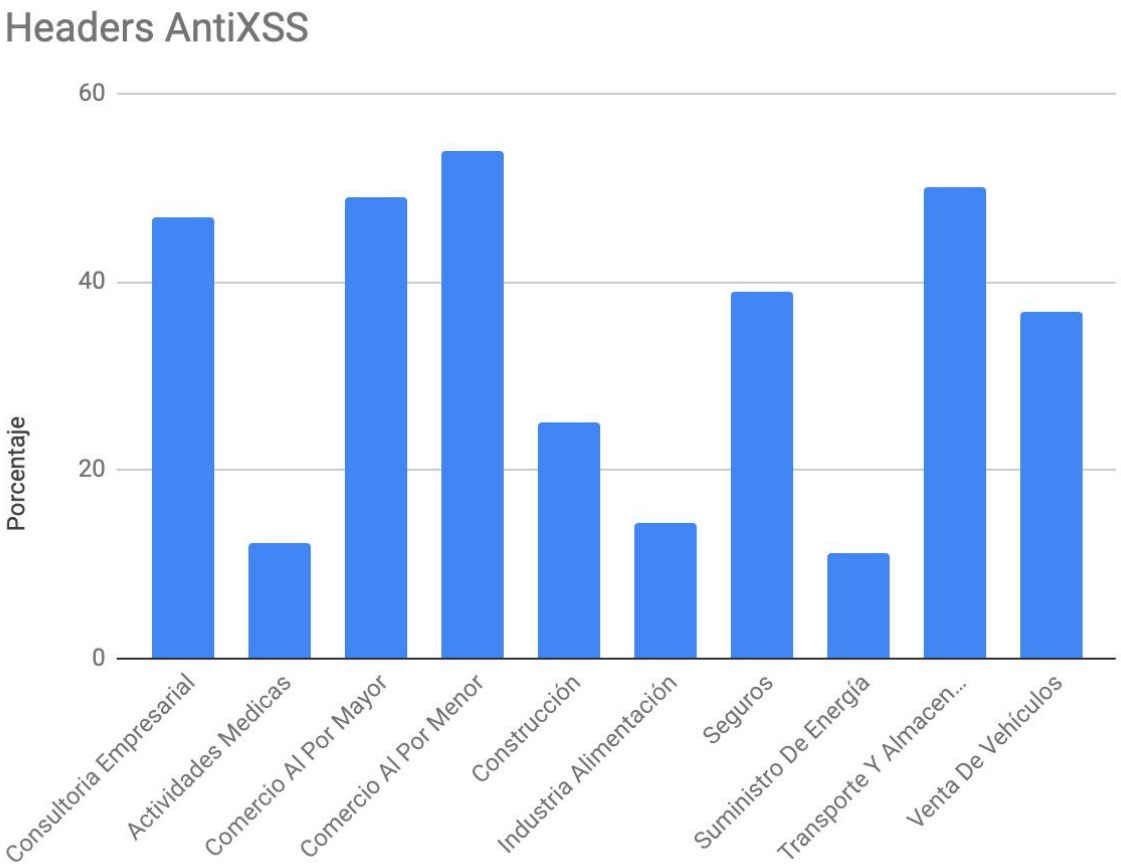
Estado de seguridad de servicios web

En este apartado se muestran los resultados obtenidos al analizar la configuración de los servidores web en cuanto a cabeceras de seguridad de refiere.

Los servidores web han ido añadiendo a lo largo del tiempo diversas capacidades de seguridad que el propio protocolo HTTP no incluía por defecto. Muchas de estas capacidades de seguridad se implementan mediante cabeceras de seguridad. La finalidad de estas cabeceras es ofrecer un mayor nivel de seguridad a los usuarios. Gracias a estas capacidades, navegar por internet es más seguro cada día. Algunas de las protecciones ante ataques que ofrecen las cabeceras de seguridad son:

- Protección ante ataques Cross-Site Scripting.
- Protección ante ataques de Clickjacking (Secuestro de clic).
- Asegurar que la comunicación sea sobre TLS/SSL mediante el estándar HSTS (HTTP Strict Transport Security).

La configuración de un servidor para el uso de cabeceras de seguridad es relativamente sencilla de implementar, sin embargo, resulta preocupante que los porcentajes obtenidos en este estudio sean tan altos. **Cuatro de los diez sectores superan el 40% de afectación**.



Estos datos son indicativos de la necesidad de mejorar las políticas de seguridad. Las organizaciones deben considerar la protección por los usuarios como clave y debe ser abordada por parte de la estrategia de seguridad de forma directa y clara..

Conclusiones

Tras el análisis de la diversa información obtenida durante la realización del estudio, la principal conclusión a la que se puede llegar es que **las organizaciones presentan un número demasiado elevado de fallos de seguridad** en sus activos expuestos a internet.

Si bien las vulnerabilidades aquí presentes no son categorizadas de nivel crítico, sí se trata de aspectos que deben ser solucionados de cara a mejorar el nivel de seguridad de las organizaciones. Cada día aumenta la probabilidad de sufrir un ataque procedente de internet, y es vital no dar facilidades a ataques automatizados.

Existen multitud de bots y agentes maliciosos en internet que buscan constantemente estos y otros fallos de seguridad con el fin de explotarlos y aprovecharlos. Es fácil imaginar que **diversos agentes maliciosos cuenten con un listado de activos de entidades españolas junto con una relación de fallos de seguridad** que les afectan, con el fin de explotarlos en algún momento.

Es importante destacar también que la mayoría de fallos de seguridad presentados en este informe no requieren de complejas soluciones técnicas. Es de esperar, por tanto, que **la presencia de estas vulnerabilidades se deben al desconocimiento de las mismas** o de la ausencia de un plan definido para su corrección.

Metodología del estudio

Este informe ha sido desarrollado usando infraestructura controlada por el servicio MrLOOQUER Rating contando exclusivamente con métodos de recopilación de información y fuentes propias. No se ha contado con ninguna fuente de información externa.

Número de organizaciones y sectores analizados

Este informe incluye información agregada de más de 500 organizaciones de 10 sectores distintos. Algunas cifras del número de pruebas que se han realizado son:

Números de dominios descubiertos y atribuídos a entidades	65.115
Número de direcciones IP descubiertas y atribuidas a entidades	40.320
Puertos abiertos detectados	160.204
Número total de ocurrencias de seguridad detectadas	69.081

Descubrimiento de activos

El proceso de descubrimiento se realiza con el motor de descubrimiento que ha desarrollado MrLOOQUER. Se trata de un proceso completamente autónomo basado en un mínimo de información. Esa información se denomina semilla y para realizar este informe se ha utilizado el dominio principal de cada compañía analizada.

Análisis de seguridad

El análisis de seguridad realizado sobre los activos descubiertos relacionados con cada entidad se realiza mediante una serie de comprobaciones **no intrusivas** realizadas desde las sondas desplegadas en internet de MrLOOQUER. Estas comprobaciones tienen como fin detectar diversos problemas de seguridad fácilmente detectables también por un agente malicioso en internet.

La comunicación que realiza las sondas de MrLOOQUER sobre los sistemas bajo análisis sigue siempre los estándares definidos por el IETF o W3C. Es decir, se genera un tráfico similar al que cualquier otro agente legítimo en internet podría generar.

Las comprobaciones de seguridad realizadas sobre los activos para la generación de este informe se agrupan en las siguientes categorías.

- Seguridad web
- Puertos inseguros
- Correo electrónico
- Análisis de gestores de contenidos CMS
- Cifrado inseguro
- Vulnerabilidades conocida

Acerca de MrLOOQUER Rating

MrLOOQUER Rating es una solución que permite descubrir y monitorizar la superficie de ataque de los activos expuestos a internet para que las organizaciones puedan medir su nivel de riesgo ante ciberataques. Esto se realiza de forma automática y continua mediante una serie de comprobaciones pasivas que permiten detectar debilidades de los activos (IPs y dominios) expuestos a Internet.

Los productos MrLOOQUER cuentan con una infraestructura desplegada en Internet que realiza millones de chequeos todos los días sobre elementos expuestos en la red. La solución dispone de algoritmos de descubrimiento de activos que permiten detectar sistemas no inventariados y elementos que puedan estar mantenidos por terceros pero que están relacionados con el cliente, combatiendo así el Shadow IT.

La solución cuenta con un sistema de alertas y notificaciones configurables que permiten poner foco sobre los eventos más importantes y ayudar a priorizar en función del riesgo.

MrLOOQUER ofrece la posibilidad de integrar de forma inmediata cualquier nube Cloud con la plataforma de análisis pudiendo tener información en tiempo real de todo lo que se expone en la nube.

Se ofrece un portal web que permite visualizar y gestionar eficientemente la información para priorizar y afinar los procesos de análisis de riesgos.

https://www.mrlooquer.com - https://blog.mrlooquer.com - hi@mrlooquer.com - @mrlooquer