

Estado de ciberseguridad

SICURATE

BASIC

Fecha: 11 de Diciembre de 2021 a las 19:36

Análisis para ejemplo.com

Resultado 73 / 200

Valoración global



Configuración web

HTTP Headers

B

Servidor

Ports

D

Server software

C

Infosec

SSL Configuration

A

SSL Certificates

B

DNS

SPF

A+

DMARC

A+

DNSSEC

C

MX

B

Índice / Tabla de contenidos

Información

- Definición de los elementos analizados

2

¿Necesita más detalles? Contrate [aquí](#) su informe **PRO** obtendrá información específica sobre qué es lo que está fallando para que sus técnicos puedan solventarlo.

Definición de los elementos analizados



DNS

Las configuraciones del DNS aseguran las identidades del usuario y de la empresa. Una buena configuración del DNS ayuda a evitar ataques de suplantación de identidad (phishing) en el que los atacantes podrían mandar correos electrónicos en su nombre. De esta forma, el atacante puede conseguir información reservada, información de los usuarios o comprometer el acceso a la infraestructura de su empresa.

Registros SPF (*Sender Policy Framework* o Marco de Políticas del Remitente):

SPF es un protocolo de autenticación de correo electrónico que permite especificar quien puede enviar emails desde un determinado dominio. Estos registros identifican los servidores de correo autorizados a enviar correo electrónico en nombre de un dominio, garantizando que solo los hosts autorizados puedan enviar correo electrónico en nombre de una empresa al proporcionar a los servidores de correo receptores la información que necesitan para rechazar el correo enviado por hosts no autorizados.

Registros DMARC (*Domain-based Message Authentication, Reporting, and Conformance* o Autenticación de mensajes, informes y conformidad basada en dominios):

Es un protocolo de correo electrónico que permite interceptar emails de suplantación de identidad: phishing. Cuando se publica para un dominio, controla lo que sucede si un mensaje no supera las pruebas de autenticación, es decir, el servidor del destinatario no puede verificar que el remitente del mensaje sea quien dice ser, por ejemplo: no hacer nada, poner en cuarentena el mensaje o rechazar el mensaje.

DNSSEC (*Domain Name System Security Extensions* o Extensiones de Seguridad para el Sistema de Nombres de Dominio):

Una de las piedras angulares sobre las que se sustenta Internet es el sistema de nombres de dominio DNS, que tiene como objetivo traducir los nombres de dominio que utilizan los usuarios en direcciones IP que puedan interpretar las máquinas. La utilización de DNSSEC aporta una capa extra de autenticidad sobre los datos enviados, evitando ataques de suplantación tipo phishing, y aumenta la protección frente a ataques de observación e interceptación del tráfico.

MX (*Mail Exchange* o Intercambio de correo):

Esta característica permite configurar los servidores de correo para su dominio de acuerdo con el protocolo de correo electrónico SMTP. Una configuración robusta en este campo permite mantener la comunicación segura entre los clientes de correo (MUS) y el servidor encargado de su envío (MSA). Esta configuración será en vano si DNSSEC no está correctamente configurado, puesto que un atacante podría cambiar las direcciones de correo (MX) para interceptar los mensajes entrantes.



Infosec

La categoría de seguridad de la información mide los factores que aseguran la confidencialidad de la información intercambiada entre los usuarios y el servidor. Una configuración con baja puntuación en esta categoría indica un cifrado débil o una mala configuración que podrían exponer el contenido de las comunicaciones.

Certificado SSL (*Secure Socket Layer* o Capa de Conexión Segura):

Un certificado digital consta de un par de claves criptográficas que otorga confidencialidad a la información transmitida y garantiza su integridad:

- Protección de la información en tránsito: Se garantiza el cifrado en todas las comunicaciones entre el navegador de un cliente y el sitio web, siendo ininteligibles para un tercero.
- Identificación del sitio web: El certificado digital se emite para un dominio concreto, es su seña de identidad en internet.
- Integridad de la información en tránsito: Si se produjera alguna modificación malintencionada o pérdida en la información intercambiada entre cliente y servidor se podría identificar y descartar.
- No repudio: Una transmisión de datos considerada válida no se puede rechazar, ya que el protocolo garantiza que ambos extremos son legítimos y que se mantiene la integridad de la misma.

Es importante destacar que sea cual sea el certificado empleado, este otorgará confidencialidad a la información transmitida y además garantizará su integridad.

Configuraciones SSL:

Las configuraciones incorrectas o débiles de los servicios que provee un Certificado SSL, pueden hacer que los servidores sean vulnerables a ciertos ataques, y permitir que se tenga acceso a información confidencial. Certificados en versiones SSL o inferiores a TLS 1.2, ya no satisfacen las necesidades de seguridad de las organizaciones al no implementar criptografía sólida para proteger, por ejemplo, los datos de pago a través de canales de comunicación públicos o no confiables.



Configuración web

La configuración de la página y el servidor web son importantes a la hora de reducir la superficie de ataque. Una mala configuración provee a los atacantes de herramientas y facilidades para perpetrar distintos ataques y lograr la entrada al servidor.

HTTP Headers (Cabeceras de las aplicaciones Web):

Los encabezados de la aplicación web analizan los campos relacionados con la seguridad en la sección del encabezado de las comunicaciones entre los usuarios y una aplicación. Contienen información sobre los mensajes, determinan cómo recibir mensajes y cómo los destinatarios deben responder a un mensaje.

Al igual que un membrete comercial, los encabezados explican a dónde va el mensaje y de quién es, la fecha de envío, el tipo de mensaje y otras opciones de configuración. Están incluidos en todas las comunicaciones de ida y vuelta entre aplicaciones. Los servidores web y las aplicaciones conectadas a la web deben cumplir con un determinado conjunto de estándares de lenguaje (comunicación) cuando se envía información a través de Internet. Estas definiciones de lenguaje se denominan "protocolos".

Los encabezados obligatorios son importantes para evitar que los ataques de comunicación entre aplicaciones tengan éxito. El uso de encabezados de aplicaciones web adecuados a través de Internet garantiza que las comunicaciones sean sólidas contra ataques diseñados para aprovechar la ambigüedad (detalles de la comunicación que no se definen explícitamente), y cubren los riesgos de seguridad que se presentan a los usuarios de las aplicaciones web.



Servidor

El servidor alberga la página web y es esta la principal puerta de entrada a posibles atacantes, aunque el atacante puede utilizar técnicas de enumeración para detectar otros servicios y explotarlos. Una mala configuración en esta categoría supone que el atacante puede tener acceso a los servicios que residen en el servidor y puede identificar vulnerabilidades,

configuraciones erróneas o contraseñas por defecto para entrar y tomar control del servidor, pudiendo secuestrar la información o generar problemas de funcionamiento (inconvenientes para la continuidad del negocio).

Ports (Puertos de Comunicación):

Los puertos son puntos de acceso virtuales para que el software se comunique a través de la red y son una característica estándar de los sistemas operativos, y hay hasta 65.535 puertos. Además, la mayoría de los sistemas operativos no bloquean deliberadamente el uso de los puertos disponibles de forma predeterminada. Ciertos puertos deben estar abiertos para admitir las funciones comerciales normales: el correo electrónico, la navegación web segura y la búsqueda de impresoras u otras computadoras en la red local de una empresa. La disponibilidad de los puertos se puede controlar con un firewall. Si bien es muy poco probable que una empresa no tenga puertos abiertos, cuantos menos puertos estén expuestos a Internet, menos "puertas" habrá abiertas para recibir ataques.

Server Software (Software de los Servidores):

Si el software del servidor no corresponde a una versión actualizada, no es compatible, o no está soportado por el fabricante, presenta problemas de seguridad que no podrán ser resueltos. Solo las versiones de software compatibles reciben la atención del equipo de desarrollo de software del proveedor, y cuando se descubren errores o vulnerabilidades generan parches de actualización que previenen los fallos de seguridad detectados. Los fallos de seguridad se utilizan para crear una imagen rica sobre el software utilizado por una organización, y detectar vulnerabilidades que son aprovechadas para extorsionar encriptar la información o interrumpir la continuidad del negocio.

¿Necesita ayuda para mejorar su estado de ciberseguridad? [Contacte](#) con nosotros para obtener más información sobre los servicios que se ofertan para reducir su superficie de ataque, protegerse de ataques y mejorar su imagen.