Limitación de la navegación hacia Internet mediante Listas Blancas como medida para reducir la superficie de exposición

Abstract: se debe considerar la limitación de la navegación y conectividad hacia Internet, solo a aquellos sitios webs relacionados con el puesto de trabajo, como medida a implementar para reducir la superficie de exposición de los sistemas y dispositivos de las entidades en un escenario marcado por el aumento de las campañas de *phishing* y las excepcionales situaciones de teletrabajo.

Contenido:

1. CONTEXTO 1
2. ANTECEDENTES 1
3. LISTAS BLANCAS 2
3.1 LUGARES DE APLICACIÓN DE LISTAS BLANCAS 2
3.1.1 Firewall y proxies corporativos 3
3.1.2 DNS 3
3.1.3 Analizadores de correo electrónico 3
3.1.4 Otros factores 4
4. MODELO DE FORMULARIO DE SOLICITUD DE LISTA BLANCA 4

1. CONTEXTO

En la actualidad se están dando continuas campañas de *phishing* y ataques cibernéticos tanto dirigidos como genéricos. La gran mayoría de estos ataques necesita que se establezca una conexión remota con un ordenador ajeno a la entidad y disponible a través de Internet, ya que sin esta comunicación el ataque se detiene y no progresa.

Existen muchas páginas web que, mediante anuncios o correos electrónicos maliciosos, infectan a los usuarios. Al estar muy bien diseñados estos sitios web son muy complicados de identificar, incluso para el personal que se dedica a la seguridad.

Otros vectores de ataque los constituyen las redes sociales y los correos electrónicos que, mediante publicidad, permiten acceder a servidores y páginas web con contenido ficticio, pero que incluyen código dañino para infectar a los dispositivos.

Por todo ello, se debe considerar que únicamente se permita a los usuarios navegar hacia sitios web relacionados con el puesto de trabajo. Los servidores de las entidades deberían ser muy restrictivos en los servicios que exponen y no tener habilitada la navegación durante escenarios marcados por campañas de *ransomware* o *phishing*.

2. ANTECEDENTES

Durante el escenario delimitado por los ciberataques relacionados con *Struts2* se formateaban y eliminaban los recursos de almacenamiento de servidores vulnerables

expuestos a Internet. El problema identificado consistía en que los servidores podían comunicarse libremente con dispositivos y sitios webs de Internet, facilitando a los atacantes la explotación de la vulnerabilidad asociada.

Como caso de éxito, se advirtió que, al aplicarse medidas de restricción de acceso a Internet, se detuvieron los ataques y pudieron llevarse a cabo las actuaciones oportunas para mejorar los niveles de seguridad.

3. LISTAS BLANCAS

La limitación de la navegación y conectividad hacia Internet se puede realizar mediante la aplicación de listas blancas en los dispositivos perimetrales. Este método se puede aplicar de distintas maneras:

- Cierre total del acceso web, que irá abriéndose según se reciban peticiones expresas solicitando navegar a ciertas páginas web o acceso a ciertos dominios. Para ello, se podría utilizar un formulario de solicitud de lista blanca para remitir la petición a los equipos de seguridad.
- Revisión de los accesos de las últimas semanas y comprobación de cuáles son legítimos o acordes con las labores del usuario o de la entidad. Habitualmente, los sitios webs necesarios para el puesto de trabajo suelen ser los más accedidos.

La revisión de las páginas, servidores y aplicaciones web con más acceso en las semanas previas a una situación excepcional, como el confinamiento debido al Covid-19, sirve para disponer de patrones de acceso relacionados con una situación laboral cotidiana y puede ser una estrategia para acelerar a la implantación de listas blancas.

3.1 LUGARES DE APLICACIÓN DE LISTAS BLANCAS

Por su naturaleza, las listas blancas se aplicarían directamente en los *firewalls* de la entidad, si bien se puede acentuar y mejorar su efecto mediante la inclusión de listas blancas en los servidores DNS de la entidad, controlando las peticiones de resolución de nombres.

Se ha de tener en cuenta que los atacantes pueden tener una vía de escape al filtrado en el servicio DNS, al utilizarse mecanismos de consultas de DNS sobre HTTPS (DoH) o sobre TLS (DoT). Asimismo, se dispone de una vía de escape adicional si las comunicaciones se realizan directamente mediante direcciones IP, sin hacer uso del servicio DNS.

Si se usaran estos dos (2) últimos mecanismos de evasión del filtrado mediante DNS, sería necesario que los *firewalls* impidiesen la conexión. **Por ello, la aplicación de las listas blancas debe ser conjunta entre *firewalls* y servicio DNS.**

3.1.1 Firewall y proxies corporativos

Los *firewalls* modernos incluyen la funcionalidad de bloquear/permitir directamente dominios, pero se recomienda añadir las direcciones IP por si se utilizase alguna técnica de resolución mediante DNS sobre HTTPS o TLS, o conexión directa mediante direcciones IP.

La recomendación sería aplicar la regla de denegación de todo el tráfico por defecto e ir permitiendo progresivamente las conexiones legítimas o necesarias.

Antes de aplicar esta medida, se recomienda hacer una revisión de las conexiones más necesarias y comenzar por su aplicación en la navegación web de los usuarios.

- Limitar las conexiones de DNS únicamente a los servicios o dominios autorizados por la organización, preferiblemente utilizando servidores DNS propios e internos a la entidad.
- Revisar si las páginas web solicitadas son legítimas o contienen contenido lesivo para la seguridad de la entidad.
- Registrar las máquinas que intentan acceder a direcciones IP no permitidas, por si el dispositivo que origina dicha conexión se encuentra infectado.

3.1.2 DNS

En el caso del servicio de DNS, se recomienda:

- Limitar la resolución de webs no necesarias para el desempeño laboral, pudiendo comenzar por denegar toda resolución web externa.
- Únicamente se permitirá la resolución de los lugares aprobados por la entidad en sus listas blancas.

Una vez aplicadas estas medidas, se deben limpiar las caches de los servidores DNS para eliminar resoluciones realizadas en el pasado.

La dirección IP proporcionada como respuesta en las resoluciones DNS no permitidas puede ser la asociada a *localhost*, 127.0.0.1 o a algún *sinkhole* que tenga la entidad para así además poder registrar los dispositivos que acceden.

En este sentido, se considera fundamental tener el registro de los dispositivos que intentan acceder a sitios no legítimos, puesto que puede ser un indicativo de estar infectado o de haber recibido algún enlace malicioso y por ello, se deben revisar.

3.1.3 Analizadores de correo electrónico

En el caso del correo electrónico, se recomienda:

- Limitar la recepción de ficheros ejecutables tanto por su extensión como por la cabecera del fichero (por ejemplo, MZ/MZP en el caso de ficheros ejecutables).

- Avisar de la recepción de correos con ficheros adjuntos ofimáticos que contengan macros y ponerlos en cuarentena.
- Activar la configuración de SPF (Sender Policy Framework) para asegurar la procedencia de los correos.
- Activar, si es posible, DKIM (Domain Keys Identified Mail) y DMARC (Domain-based Message Authentication, Reporting & Conformance).

3.1.4 Otros factores

En la actualidad, muchos usuarios se encuentran teletrabajando. Si acceden a la entidad mediante una conexión VPN se limitará el acceso hacia Internet desde la salida principal del propio organismo.

En función de si las entidades han habilitado o no la configuración de *split tunneling* en el servicio DNS asociado a la VPN, se puede limitar la navegación web de los usuarios desde su ubicación remota mientras se encuentran conectados a través de la VPN. Para ello, se debe deshabilitar el *split tunneling*, de forma que todo el tráfico se curse por dentro de la VPN.

En caso de no disponer de la posibilidad de deshabilitar *split tunneling*, podría ser interesante hacer uso de una solución de filtrado tipo Pi-hole (aplicación para bloqueo de anuncios y rastreadores en Internet).

Por otro lado, casi todos los usuarios disponen de acceso a Internet propio o en el teléfono móvil desde donde pueden realizar las conexiones asociadas a su vida personal, independizándose así de las tareas propias de conectividad que se requieren con la entidad para el ámbito estrictamente laboral.

De ser posible, se recomienda hacer uso de servidores DNS para la resolución de nombres con soporte para DNSSEC (Domain Name System Security Extensions) con el objetivo de que se pueda verificar la autenticidad de las respuestas asociadas al servicio DNS.

Se debe tener en cuenta que para aquellos servicios que hacen uso de redes de distribución de contenidos CDN (Content Delivery Networks), el filtrado por dirección IP puede ser muy complejo o inabordable.

4. MODELO DE FORMULARIO DE SOLICITUD DE LISTA BLANCA

Se debe disponer de un formulario para ser cumplimentado por los peticionarios y enviado a los equipos de seguridad que permita realizar solicitudes expresas de navegar a ciertas páginas web o disponer de acceso a ciertos dominios.

Solicitud de Acceso hacia Internet (Lista Blanca)

Persona solicitante: _____

Teléfono de contacto: _____

E-mail de contacto: _____

Responsable que autoriza la petición:

_____

Páginas, servidores, aplicaciones web o dominios (separadas por *intro* o ",") a los que solicita acceder:

_____

Direcciones IP a las que solicita acceder (separadas por *intro* o ","):

_____

Categoría laboral de las páginas web o dominios a los que desea acceder (agrupadas por categorías):

_____

Período de acceso (en caso de acceso puntual, indicar horas o días necesarios):

_____

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.04.08 23:44:37 +02'00'