RECOMENDACIÓN DEL GRUPO DE TRABAJO DE SEGURIDAD Y AUDITORÍAS DE CRUE-TIC PARA LA SECURIZACIÓN DEL PERÍMETRO EN UNIVERSIDADES

Elaboración de la propuesta / Grupo de trabajo de Seguridad y Auditorías de CRUE-TIC

Objetivo del documento / Justificar la necesidad de aplicar políticas de seguridad restrictivas al perímetro de las redes universitarias y elaborar recomendaciones de securización del perímetro.

MOTIVACIÓN DE LA APLICACIÓN DE POLÍTICAS DE SEGURIDAD PERIMETRAL

Los atacantes aprovechan cualquier tipo de debilidad en materia de ciberseguridad de las organizaciones con el objetivo de acceder y manipular los recursos informáticos de la institución. Los dispositivos de cabecera de las universidades son continuamente analizados por atacantes mediante escaneos masivos de puertos de forma indiscriminada y automatizada en busca de diferentes vulnerabilidades en los servicios accesibles desde Internet, especialmente en servicios Web. La conectividad global de Internet favorece la dispersión geográfica de los atacantes que en muchos casos disponen de más recursos para conseguir sus fines que las universidades para defenderse.

Por ello, es de vital importancia y cuestión estratégica minimizar la superficie de exposición a Internet de las universidades. Esto se alinea con dos de los principios básicos del Esquema nacional de Seguridad (ENS):

Prevención, reacción y recuperación (art. 7) que, entre otros aspectos indica que "Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición."

Líneas de defensa (art. 8): establecer múltiples capas de seguridad para reducir la probabilidad de que el sistema se vea comprometido en su conjunto

A modo de ejemplo se han detectado en algunas de nuestras universidades las siguientes circunstancias que pudieran ser explotadas por los atacantes si no se aplican políticas y filtros que eviten estas prácticas:

Hay universidades en las que la configuración software de los puestos de trabajo y servidores no está estandarizada y la responsabilidad sobre el bastionado recae sobre el propio usuario del equipo. En consecuencia, se producen situaciones en las que no se actualizan los sistemas operativos ni el software de estos equipos e incluso pueden existir aplicaciones no permitidas, vulnerables o incluso infectadas, quedando expuestos a la explotación de las vulnerabilidades desde el exterior de la Universidad, a la vez que ponen en riesgo al resto de equipos internos que comparten la red.

En las redes universitarias se instalan equipos y servicios accesibles desde Internet sin la supervisión o conocimiento de los Servicios Informáticos. En estos casos, se corre el riesgo de que no se contemplen las las mínimas medidas de seguridad en su despliegue, ni se mantengan con el paso del tiempo. En otros casos se aplican parcialmente en su instalación, pero se descuida su mantenimiento.

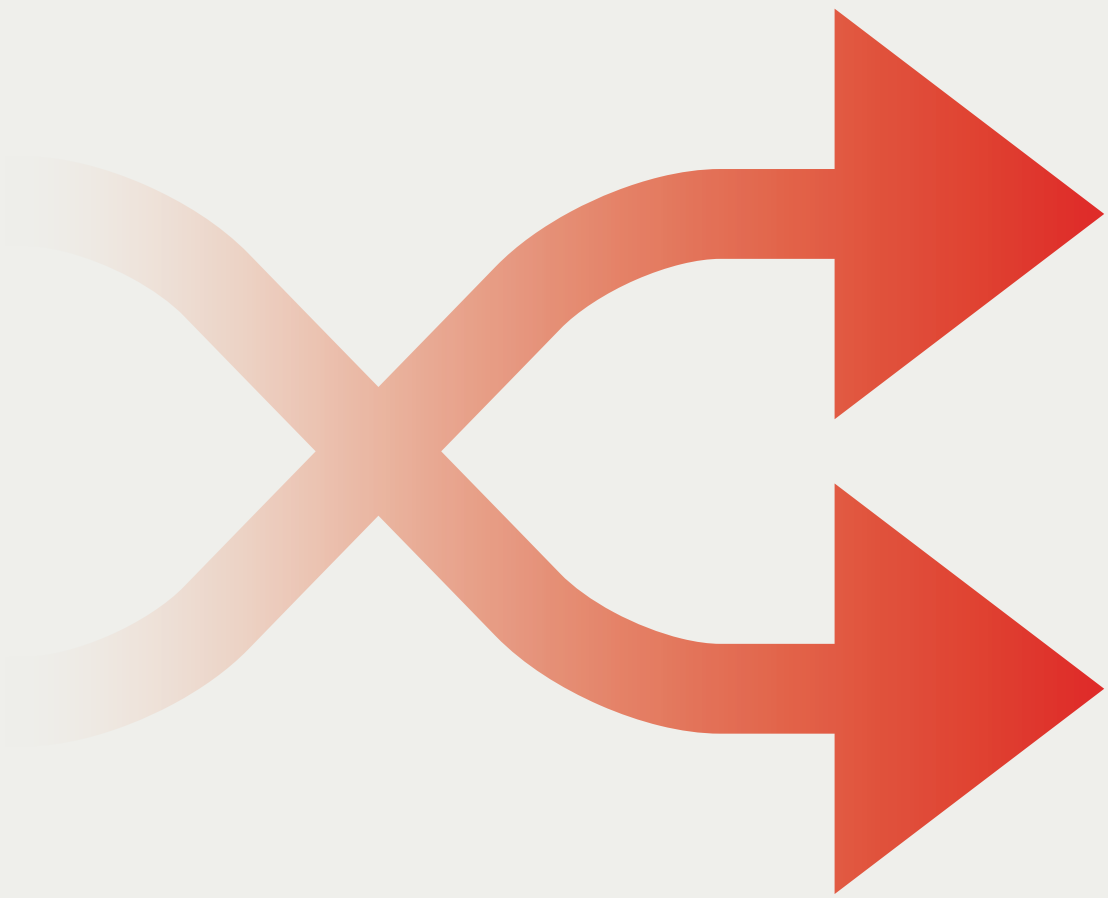
La introducción de dispositivos conectados (Arduino, Raspberry, dispositivos de control industrial y en general dispositivos IoT), cuyas actualizaciones de sistema operativo y parches no se aplican, presentan vulnerabilidades y generan desconfianza en el ámbito de la seguridad.

Existen también universidades que utilizan direccionamiento IP público en la conexión de los puestos de trabajo de los usuarios (PDI, PAS, Aulas) así como para equipos de impresión, aumentando considerablemente el riesgo de exposición.

Estas situaciones reales ponen de manifiesto la necesidad de aplicar medidas de protección en los sistemas informáticos universitarios, dotándolos de los recursos adecuados e implantando políticas que filtren y minimicen la superficie de exposición de nuestros puestos de trabajo, dispositivos y sistemas de información conectados a Internet.

JUSTIFICACIÓN DEL CAMBIO

Aspectos a tener en cuenta



1. CUMPLIMIENTO NORMATIVO

El Esquema Nacional de Seguridad (Real Decreto 3/2010), en adelante ENS, en el Artículo 22 "Prevención ante otros sistemas de información interconectados" hace referencia a la protección del perímetro, en particular si la organización se conecta a redes públicas. En el anexo II de Medidas de seguridad la medida [mp.com.1] "Perímetro seguro" establece que "...se dispondrá un sistema cortafuegos que separe la red interna del exterior para Sistemas de Información a partir del nivel BAJO. Todo el tráfico deberá atravesar dicho cortafuegos que sólo dejará transitar los flujos previamente autorizados".

El REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos establece, en el considerando (49), "... el interés legítimo del responsable del tratamiento para tratar datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, ... y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, ... En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas."

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales establece en la Disposición adicional primera, "Medidas de seguridad en el ámbito del sector público" que las Administraciones Públicas "... deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad."

2. OPERATIVA DE LOS SERVICIOS CORPORATIVOS

Son múltiples las consecuencias de tener equipos y servicios vulnerables expuestos a Internet: pérdida de reputación de la institución, incumplimiento de la legislación, pérdidas económicas por robo o estafa, inclusión en listas negras por ataques desde equipos infectados de la Universidad hacia el exterior, carga de trabajo extra e indisponibilidad de los servicios todo ello provocado por los múltiples incidentes de seguridad.

3. RECOMENDACIONES DEL CCN-CERT

Guía CCN-STIC 811 Interconexión en el ENS.
CCN-STIC-820 Protección contra Denegación de Servicio.
Guías CCN-STIC serie 600 para configuración de equipos de Comunicaciones y Cortafuegos de distintos fabricantes

RECOMENDACIONES PARA LA PROTECCIÓN PERIMETRAL DE LA RED UNIVERSITARIA

1. Acceso a servicios públicos

La política de seguridad por defecto debe ser rechazar cualquier conexión que no esté expresamente permitida desde la zona internet hacia las zonas o redes internas. **Solo deben estar accesibles desde Internet aquellos servicios que sean considerados como públicos.** Tendrán esta consideración tanto los sistemas de información institucionales que ofrezcan información o servicios a los ciudadanos, como aquellos servicios que por necesidades de los usuarios de la Universidad deban ser accesibles desde Internet. Este último caso debe reducirse a lo mínimo imprescindible y limitar con políticas de seguridad tanto el origen como el destino siempre que sea posible. Se denegará el tráfico al resto de equipos (direcciones IP), sean servidores o equipos de usuarios, y servicios (puertos TCP/UDP). De esta forma se reduce la ventana de exposición y se reducen los riesgos a que están expuestos los recursos TI de los riesgos y amenazas que supone estar conectado a Internet.

2. Cortafuegos

Uso de cortafuegos de nueva generación (capa 7). Recomendaciones de configuración:

Configuración de zonas de seguridad. Se debe configurar una zona de seguridad para cada red o redes que tengan un nivel de seguridad similar. Típicamente habrá, al menos, tres zonas: internet, una DMZ (servicios públicos) y una intranet (red de usuarios). Sin embargo, puede haber muchas más zonas de seguridad en función de la arquitectura de red, los servicios de cada institución y los requerimientos de seguridad de la información tratada por los equipos conectados. El tráfico entre zonas por defecto está denegado y debe ser permitido expresamente en función de las necesidades, En especial, las políticas de seguridad sobre las redes DMZ deben garantizar que solo se permiten conexiones entrantes a aquellos servicios declarados; de igual forma deben aplicarse políticas restrictivas a las conexiones dirigidas hacia la zona internet y a otras zonas de seguridad públicas o internas.

Alta disponibilidad. Es la capacidad de que el servicio funcione correctamente sin fallas o interrupciones ante un fallo del firewall. Supone la existencia de 2 firewalls configurados en clúster. El clúster puede ser configurado en modo activo/pasivo o activo/activo, pero en ambos casos ante la caída de un firewall activo, el otro se hace cargo del servicio de forma automática y transparente.

Activación de las funcionalidades básicas del cortafuegos:

Filtrado de tráfico malicioso. En base a listas de reputación, debe rechazarse el tráfico que pueda suponer un riesgo para la institución desde sitios que estén distribuyendo malware o que estén identificadas como hostiles.

Filtrado de botnets y servidores de comando y control. En base a listas de reputación y suscripción a servicios de listas negras deben filtrarse las conexiones con infraestructura de botnets conocidas (dominios, servidores, etc.) y especialmente con sus servidores de comando y control (C&C).

Activación de IPS. Todo el tráfico que atraviesa el firewall debe ser analizado por su módulo de prevención de intrusiones (IPS por sus siglas en ingles). Si una conexión es detectada como un ataque, el firewall debe estar configurado para rechazar dicha conexión.

Inspección SSL de los servicios críticos. La inspección SSL es una tecnología que permite desencriptar y analizar el tráfico en busca de ataques y contenido malicioso. Debido a que normalmente los servicios críticos de las instituciones se ofrecen cifrados, es necesario habilitar la inspección SSL de los mismos para que la protección de IPS sea efectiva.

Filtrado por aplicación. Los firewalls de nueva generación analizan a un nivel profundo (deep packet inspection) el tráfico identificando el tipo de aplicación. Se debe, en la medida de lo posible, realizar políticas de seguridad por aplicación y no por puerto para evitar el tráfico de determinadas aplicaciones por puertos no estándar.

Prevención DoS1. Si bien los firewalls de nueva generación no son dispositivos especializados para este propósito, sí tienen módulos anti-DoS. Deben configurarse, adaptados a los perfiles de trafico de cada institución por dos motivos: en primer lugar, para proteger a los servidores que están en las zonas de seguridad interiores; y en segundo para protegerse a sí mismos y seguir teniendo recursos para realizar su función.

Bloqueo de escaneos. Los firewalls de nueva generación disponen de capacidades para detectar y bloquear la actividad de escaneo.

QoS. Los firewalls de nueva generación pueden realizar tareas para garantizar la calidad de servicio de determinadas aplicaciones o para limitar el uso de otras. Debe usarse esta capacidad para garantizar la disponibilidad de los servicios públicos y las políticas de uso aceptable de las redes académicas.

3. Acceso remoto

Acceso Remoto. Salvo a los servicios públicos, el acceso a las zonas de seguridad internas de la red de la institución debe realizarse a través del Servicio de VPN Corporativo no permitiendo el uso de otras herramientas que puedan, intencionadamente, evitar los controles de seguridad perimetrales (Ej, TeamViewer, VNC, etc.).

4. WAF

Uso de WAF. Los Web Application Firewall son capaces de supervisar, filtrar y bloquear tráfico HTTP hacia y desde aplicaciones web. Aportan visibilidad y aunque su configuración puede llegar a ser compleja, pueden ser barreras muy efectivas frente a ataques a las aplicaciones web críticas.

5. Proxy Inverso

Uso de Proxy Inverso. Permite entre otras ventajas anonimizar la existencia de los servidores y sus características a los clientes que hacen peticiones a los servicios, así como tareas de balanceo de carga. También puede contener funcionalidades de protección web (WAF) y cifrado SSL de las comunicaciones.

6. Securización DNS

Securización DNS. El servicio de DNS es una de las infraestructuras básicas de nuestra red. Sin un servicio DNS seguro toda nuestra red es vulnerable. Se recomienda:

Implantar DNSSEC como una medida efectiva para evitar ataques de envenenamiento de cache.

Uso de DNS firewall o RPZ para poder detectar y detener aquellas conexiones que nuestros usuarios realizan a dominios maliciosos.

Limitar la recursión a solo la red de la institución. Evitará que se usen los DNS de la institución como fuente de ataques de denegación de servicio amplificados.

Restringir el uso de DNS desde las redes internas a los servidores DNS institucionales, permitiendo proteger la resolución DNS de amenazas, así como el uso de técnicas anti-firewall.

7. Securización del correo electrónico

Securización del servicio de Correo electrónico. Se recomienda aplicar los criterios de calidad RACE de RedIris en su nivel “Avanzado” (ver http://www.rediris.es/mail/race/criterace.es.html)

8. Herramientas CCN-CERT2

Uso de servicios y herramientas del CCN-CERT2 y otros CERTs de referencia.

9. Auditorías periódicas

Realización de auditorías periódicas sobre los servicios públicos de la universidad.

RECOMENDACIONES PARA LA IMPLANTACIÓN DE MEDIDAS DE SEGURIDAD PERIMETRALES

Para la implantación de las medidas asociadas a la securización del perímetro es necesario contar con apoyo institucional (por ejemplo, del Comité de Seguridad), documentar las medidas y el impacto que supondrán en los usuarios e informar a todas las partes que se verán afectadas (usuarios, empresas, etc.).

Si bien disponer de un firewall de capa 7 para securizar el perímetro es una muy buena noticia, hay que tener en cuenta que la institución debe contar con recursos humanos suficientemente cualificados para sacarle el máximo provecho. Este tipo de firewall genera una gran cantidad de logs y alarmas que es necesario analizar periódicamente para tener una correcta visión de lo que está ocurriendo. Como consecuencia de esta visibilidad en ocasiones será necesario realizar ajustes en la configuración del firewall. Si la institución no cuenta con suficientes recursos humanos para llevar la operación del firewall, puede ser necesario valorar la externalización del servicio.

Otro punto crítico cuando se dispone de este tipo de cortafuegos es que esté dimensionado para el ancho de banda de conexión a Internet de la institución. O sea, que teniendo activadas todas las capacidades de protección, el firewall sea capaz, por ejemplo, de soportar ataques volumétricos que saturen su ancho de banda.

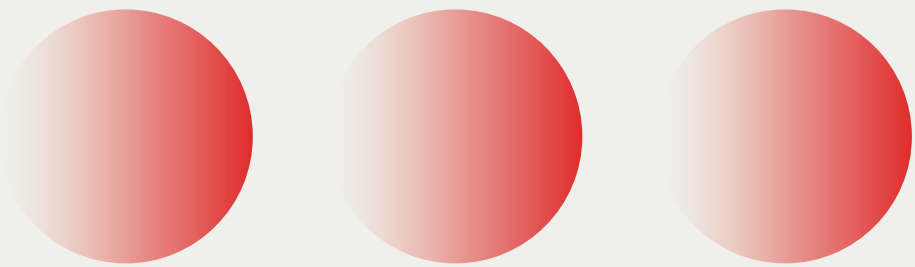
La aplicación de las medidas propuestas debe realizarse gradualmente evaluando por cada una el impacto y posibles efectos adversos y, por supuesto, teniendo preparada una marcha atrás para el caso de que la aplicación de la medida genere efectos no deseados.

Hay medidas como el filtrado de puertos que debe venir precedida, siempre que sea posible, de un estudio sobre qué puertos son utilizados por el tráfico de la organización. Además de los puertos estándar en muchas ocasiones se usan puertos no estándar para, por ejemplo, aplicaciones. Hay que tener en cuenta que, si filtramos algunos de estos puertos no estándar, es posible que haya aplicaciones que dejen de funcionar. Debe articularse un mecanismo para minimizar estos casos, permitiendo además que si llegaran a ocurrir pudieran solventarse en el menor tiempo posible.

Es crucial en la implantación de estas medidas actuar diligentemente en caso de que algo vaya mal. Para ello se hace necesario tener un contacto directo con el canal de entrada de incidencias informáticas de la institución; de forma que las incidencias reportadas por los usuarios lleguen en el menor tiempo posible a los responsables del despliegue de las medidas y puedan actuar en consecuencia para solventarlas.

Con la securización perimetral se busca reducir la superficie de exposición ante ataques a la institución. Por ello, una vez implantadas todas las medidas es necesario evaluar si efectivamente hemos conseguido disminuir dicha exposición y en qué grado. Esta información es importante de cara a justificar las medidas implantadas y el coste de las mismas ante la dirección de la institución.

OTRAS RECOMENDACIONES BÁSICAS DE SEGURIDAD



Aunque no sea objeto de este documento, se recomienda que, además de la seguridad del perímetro, las universidades dispongan de una arquitectura de seguridad interna que incluya:

Distintos niveles de cortafuegos independientes que minimicen el impacto de un ataque al firewall perimetral, de manera que, aunque un posible ataque afectara al Servicio de Acceso a Internet, no pudiera afectar al resto de servicios que se proporcionan a nivel interno (DNS/DHCP, WiFi, recursos internos, etc.).

Gestión de la seguridad en los equipos de los usuarios: utilización de soluciones de seguridad para equipos de usuarios (Endpoint); antivirus; control de acceso a la intranet (NAC); agentes de detección (y notificación) de malware y comportamientos sospechosos en dichos dispositivos; agentes de inventario; maquetación de equipos, etc. Estas herramientas deberán instalarse en todos los equipos del personal de la universidad.

Un proceso continuo que contemple la Gestión de vulnerabilidades que de forma proactiva se puedan corregir antes de que sean explotadas por atacantes. Por ejemplo, realizar auditorías y pruebas periódicas de pentesting de los activos conectados, implementar las acciones que anulen o minimicen las vulnerabilidades detectadas, sin olvidar la notificación y documentación de las mismas.

Equipamiento que permita tener la visibilidad y trazabilidad necesarias para detectar ataques dentro de la propia Universidad (como por ejemplo un SIEM).

Segmentación de redes, proxy para Servicios Corporativos, direccionamiento privado, maquetación de equipos, etc.


crue
Universidades
Españolas
TIC