Configuración de dispositivos y sistemas informáticos (Bastionado de redes y sistemas)

Seguridad perimetral. Firewalls de Próxima Generación

La seguridad perimetral corresponde a la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles.

Los elementos básicos son:

- Cortafuegos o firewalls.
- Sistemas de detección y prevención de intrusiones (IDS/IDPS).
- Pasarelas «antimalware» y «antispam».
- Redes privadas virtuales (VPN).

La mayoría de los firewalls de próxima generación (NGFW) se centra, principalmente, en permitir el control de las aplicaciones, pero no tanto en sus capacidades de defensa contra amenazas. Para compensar, algunos NGFW intentan complementar la prevención de intrusiones de primera generación con una serie de productos complementarios no integrados. Sin embargo, este enfoque no hace mucho para proteger a su empresa contra los riesgos que implican los atacantes sofisticados y el malware avanzado. Además, una vez que se produce una infección, no brindan ningún tipo de ayuda para determinar su alcance, contenerla y corregirla

rápidamente.

Seguridad de portales y aplicativos web. Soluciones WAF (Web Aplication Firewall)

Un firewall de aplicaciones web es un tipo de firewall que supervisa, filtra o bloquea el tráfico HTTP hacia y desde una aplicación web. Se diferencia de un firewall normal en que puede filtrar el contenido de aplicaciones web específicas, mientras que un firewall de red protege el tráfico entre los servidores.

Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, antimalware

(Información obtenida de INCIBE).

La gestión de la información, principal activo de nuestra empresa, tanto desde dispositivos tecnológicos como no tecnológicos se realiza desde el puesto de trabajo. El puesto de trabajo ha ido extendiéndose con la incorporación de los nuevos dispositivos tecnológicos.

Actualmente se utilizan dispositivos muy diferentes como ordenadores de sobremesa, portátiles, teléfonos móviles, tabletas, dispositivos de almacenamiento extraíbles, impresoras de red, escáneres, etc. Dentro de este escenario de riesgo es donde pueden producirse fuga de datos, pérdida de información confidencial o infecciones por malware.

Para mitigar estos riesgos, se deben establecer medidas de seguridad, adaptadas a las necesidades del puesto de trabajo, tanto de carácter organizativo como técnico. La aplicación de

estas medidas, junto a un adecuado plan de formación y concienciación de los empleados que gestionan la información desde sus puestos de trabajo, nos ayudará a proteger de manera adecuada nuestra empresa.

Más información

- https://www.jesusninoc.com/01/10/ejercicios-de-seguridad-practica-sobre-virus-en-powershell/
- https://www.jesusninoc.com/03/11/keylogger-sencillo-con-powershell/
- https://www.jesusninoc.com/03/11/enviar-datos-a-un-formulario-de-google-docs-desde-powershell/

Seguridad de entornos cloud. Soluciones CASB

CASB, Cloud Access Security Broker, es un tipo de software que tiende a proteger las aplicaciones SaaS de las empresas (Salesforce, Box…) e IaaS (OCI, AWS, Azure…) para que los datos de la organización estén seguros. CASB proporciona seguridad de datos de extremo a extremo, desde la nube hasta el dispositivo.

Seguridad del correo electrónico

(Información obtenida de INCIBE).

A la hora de gestionar información en cualquier empresa, el correo electrónico es una herramienta de comunicación básica e imprescindible. En ocasiones, puede que la empresa tenga que hacer uso de más de una cuenta de correo y a buen seguro que

serán varios emails los que envíe y reciba diariamente.

Asociado al uso de cualquier herramienta de comunicación corporativa, también para el correo electrónico, la empresa deberá tener definida una política para un uso correcto y seguro. Además deberá difundirla entre los empleados y garantizar que se cumple. De esta forma se asegurará que sus empleados puedan enviar y recibir correos con información confidencial, sin el perjuicio que podrían provocar posibles ataques. Adicionalmente, esta política marcará las acciones a llevar a cabo para proteger los buzones corporativos ante spam o correos de phishing que intenten hacerse con credenciales o suplantar la identidad de personas o entidades.

El correo electrónico es una herramienta que aporta grandes beneficios en cuanto a disponibilidad, accesibilidad, rapidez, posibilidad de envíos a varios destinatarios de varios documentos, etc., que permite agilizar gran parte de las tareas del día a día de cualquier oficina. Pero a su vez, esta herramienta es una de las fuentes más comunes de ciberataques e introducción de malware en cualquier empresa. Será muy importante que además de una política sólida de uso, se tenga presente la formación y concienciación a los empleados, ya que son los usuarios finales de las cuentas de correo.

Soluciones DLP (Data Loss Prevention)

Una solución de prevención de pérdida de datos es un sistema que está diseñado para detectar potenciales brechas de datos/ transmisiones de datos y prevenirlos a través de monitoreo, detección y bloqueo de información sensible mientras está en uso, en movimiento y en reposo.

Herramientas de almacenamiento de logs

El análisis de logs es fundamental para detectar posibles anomalías en la gestión de los sistemas, por lo tanto es necesario almacenarlos correctamente y tener unos procedimientos para acceder a ellos de forma rápida y ordenada.

Protección ante ataques de denegación de servicio distribuido (DDoS)

Un ataque de denegación de servicio, también llamado ataque DoS, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Las compañías deben protegerse de las denegaciones de servicio para que no colapsen sus sistemas.

Algunas recomendaciones generales de protección frente a DDoS:

- Implementar un sistema de detección y prevención de intrusiones (IDS/IPS).
- Medidas de protección en el hosting (donde se encuentran las webs de la empresa u otros servicios).
- Ancho de banda, cuanto más mejor.
- Redundancia y balance de carga.
- Uso de soluciones de seguridad basadas en la nube.
- Sistemas actualizados.

Más información

- https://www.jesusninoc.com/07/20/ping-flood/
- https://www.jesusninoc.com/06/02/ping-continuado-a-servidores-de-tarificacion-por-byte-consumido/

Configuración segura de cortafuegos, enrutadores y proxies

Cuando un programa de nuestro ordenador necesita acceder a Internet, establece una conexión en la que enviará o recibirá la información que le sea necesaria, desde nuestro ordenador hacia Internet o desde Internet hacia nuestro ordenador, dando lugar a conexiones entrantes o salientes.

El cortafuegos, más conocido como firewall, es una herramienta que permite gestionar qué programas pueden establecerlas y qué programas no, y qué tipo de conexiones serán permitidas.

El firewall funciona como una puerta de enlace de la red con filtro y sólo es eficaz en aquellos paquetes que deben pasar a través de ella. Por lo tanto, sólo puede ser eficaz cuando la única ruta para estos paquetes es a través del firewall.

Redes privadas virtuales (VPNs), y túneles (protocolo IPSec)

Una red privada virtual es una tecnología de red de ordenadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

Monitorización de sistemas y dispositivos

Un sistema informático puede sufrir fallos o tener

funcionamiento que puede poner en serio riesgo las funciones que desarrolla la empresa.

Para adelantarse a que ocurra un fallo, existe la monitorización que se encarga de hacer un seguimiento del estado de todo el sistema informático. El objetivo de la monitorización es asegurar que el sistema es fiable y estable, capaz de proporcionar los servicios para los que ha sido diseñado.

Más información

- https://www.jesusninoc.com/03/12/mostrar-los-procesos-que-se-estan-ejecutando-en-relacion-con-los-servicios-y-los-puertos-abiertos-tcp/
- https://www.jesusninoc.com/03/11/mostrar-los-hilos-que-se-estan-ejecutando-en-relacion-con-los-servicios-los-procesos-y-los-puertos-abiertos-udp/

Herramientas de monitorización (IDS, IPS)

DS (Intrusion Detection System) o sistema de detección de intrusiones: es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas.

IPS (Intrusion Prevention System) o sistema de prevención de intrusiones: es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva.

SIEMs (Gestores de Eventos e Información de Seguridad)

Un sistema de Gestión de Eventos e Información de Seguridad es un sistema que centraliza el almacenamiento y la interpretación de los datos relevante de seguridad.

Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: NOCs y SOCs

Los Centros de Operaciones de Seguridad, conocidos como SOC por sus siglas en inglés, están enfocados principalmente en atender cuestiones de seguridad informática para proteger los servidores, redes, dispositivos y bases de datos de una organización.

Por la otra parte, los Centros de Operaciones de Redes, conocidos como NOC; están especializados en monitorear el desempeño y detectar problemas dentro de la red digital de una empresa. Los técnicos encargados de estos centros revisan minuciosamente los puntos de entrada y salida de la red para prevenir que ocurran problemas relacionados con la conectividad y rapidez del internet de una empresa.