La vigilancia como resultado del cumplimiento, visibilidad, respuesta y acceso remoto

Abstract: hay escenarios en que los sistemas, por su origen y naturaleza, tienen grandes dificultades para cumplir con los requisitos de seguridad exigidos al tipo de información que manejan y servicios que prestan. En estos casos, es donde cobra importancia la posibilidad de implementar sistemas complementarios de vigilancia que equilibren la superficie de exposición resultante de una prevención e implementación deficitaria de medidas de seguridad.

Contenido:

1. CONTEXTO

La evaluación permanente del estado de la seguridad de los sistemas de las Tecnologías de la Información y la Comunicación (TIC) es una actividad crítica en cualquier organización.

Por ello, es preciso tratar las deficiencias de seguridad, que no son solo de tipo técnico (bugs, configuraciones erróneas, puertas traseras, etc.), sino que pueden ser de tipo humano (falta de concienciación, inexperiencia, formación inadecuada, etc.), de tipo procedimental (inexistencia de documentación, acciones incorrectas, ausencia de verificaciones, etc.) o de tipo legislativo o normativo (desviación frente a los requisitos definidos como de obligado cumplimiento).

La evolución de la superficie de exposición, ante dichas deficiencias, hace necesaria la realización de auditorías de forma regular que verifiquen el cumplimiento de los requerimientos establecidos por la política de seguridad del Sistema.

2. VIGILANCIA

El modelo tradicional basado en el concepto de perímetro, donde se protege el acceso externo a la red de usuarios y dispositivos (a los sistemas y sus recursos), y al usuario/dispositivo interno se considera de confianza, ya no es válido.

La deslocalización de los datos en distintos centros de datos y nubes, así como el acceso de terceros desde dentro (proveedores e invitados) y desde fuera (proveedores y funcionarios en formato teletrabajo) de la red hace más difícil definir un perímetro.

En esta nueva realidad por definición no se puede ni se debe confiar en el usuario y/o dispositivo (entidad) interno o externo.

Esta realidad requiere un nuevo modelo de seguridad que exija una verificación estricta de identidad para cada usuario y dispositivo que intente acceder a los recursos de una red, desde fuera y/o desde dentro de la misma, sin importar la ubicación desde la que se origina la conexión.

En este nuevo modelo la importancia de la capa de acceso/electrónica es absoluta. Las deficiencias en la configuración de la electrónica (capa de acceso) permiten al atacante contar con un eslabón débil que le permite el acceso y gobierno sobre todo lo que hay dentro de la red, poniendo en entredicho cualquier otro control y/o medida de vigilancia que se puede construir sobre ella.

3. CUMPLIMIENTO, VISIBILIDAD, REPUESTA Y ACCESO REMOTO

La prevención e implementación deficitaria de medidas de seguridad lleva asociada la adopción de medidas complementarias de vigilancia para equilibrar el ecosistema de la seguridad y en este sentido, la electrónica de red y su infraestructura asociada, todo lo conectado a dicha electrónica y sus permisos correspondientes, requieren también de medidas de vigilancia y trazabilidad.

- Deficiencias en la capa de acceso y electrónica (cumplimiento).
  - Identificar deficiencias en la configuración de la electrónica de red en base a las diferencias de la configuración actual y lo definido en el módulo de referencia mediante comparación.
  - Los resultados se integran para centralizar la evaluación con el fin de determinar el grado de conformidad con la política de seguridad del sistema de información auditado y las necesidades de mejora y corrección.
- La conectividad a la red (visibilidad).
  - Conseguir una visibilidad/perfilado de todo lo conectado a la red desde dentro (usuarios internos y externos, dispositivos e infraestructura) y desde fuera (dispositivos y usuarios en modalidad de teletrabajo/proveedores de servicios), al mismo tiempo que se dota de trazabilidad sobre todo lo conectado.
- La capacidad de respuesta ante eventos (respuesta).
  - Control de los activos en redes cableadas, Wi-Fi y redes privadas virtuales (VPN) con un punto único de decisión y aplicación de las políticas de acceso y respuesta.
  - Integración con otras soluciones de seguridad (NGFW, SIEM, etc.).
    - Asignación de privilegios y permisos específicos en la red a cada entidad/identidad (asignación de VLAN, por ejemplo).

- Ejecución de acciones de respuesta para remediar o minimizar las amenazas detectadas (por ejemplo, mediante el aislamiento de la entidad comprometida). En definitiva, políticas de respuesta ante:
  - Vulnerabilidades/protocolos afectados (ejemplo, RDP).
  - Amenazas detectadas, indicadores de compromiso y comportamiento anómalo de las entidades. Por ejemplo, peticiones DNS concretas en el ataque *Wannacry* usadas como objeto para identificar entidades comprometidas y aplicación a políticas de respuesta de las mismas.
- Política de seguridad basada en el nivel de bastionado del punto final/centro de proceso de datos.
  - El aseguramiento de las políticas de seguridad definidas por la organización en cuanto a los puntos finales y servidores.
  - Definición y aplicación de políticas de acceso en función de una postura de seguridad basado en el nivel de bastionado deseado.

- Acceso remoto seguro
  - Establecer una conexión segura y verificada de manera robusta, entre el usuario y los sistemas corporativos, monitorizando de manera continua el comportamiento de la conexión.
  - El módulo de concentración de VPN actúa como *frontend* para la finalización de túneles VPN con los clientes, mediante un agente (dispositivos corporativos y no corporativos).
  - Realización de la autenticación, autorización y auditoría contra el gestor de identidades corporativas del Organismo (Active Directory (AD), LDAP…) y permitir añadir un segundo factor de autenticación (OTP), de esta forma se mitiga el riesgo de suplantación de identidad (uso de credenciales robadas por parte de un atacante para acceder a la red).
  - Se recoge el inventario y perfilado completo del equipo. Este perfilado se podrá utilizar en las políticas de acceso a la conexión remota.
    - Adicionalmente, permite definir y aplicar políticas de acceso en función de una postura de seguridad basada en el nivel de bastionado deseado, además de otros factores (horario de la conexión, características del equipo, role de usuario, etc.).
    - Permite así una conexión segura y verificada de manera robusta entre el usuario y los sistemas corporativos.

3.1 EMMA - VIGILANCIA DE LA INFRAESTRUCTURA DE RED

EMMA es una solución encargada de la vigilancia de deficiencias en la capa de acceso y electrónica (cumplimiento), conectividad a la red (visibilidad), capacidad de respuesta ante eventos (respuesta) y acceso remoto seguro.

Esta solución está pensada para agilizar la visualización de activos en una red, su autenticación y segregación, así como la automatización de auditorías de seguridad de la infraestructura.

Con ella, el CCN-CERT pretende facilitar a las organizaciones una visibilidad completa de la capa de acceso a la red (routers, switches, puntos de acceso, controladores, etc.), un punto crucial para verificar quién o qué está conectado en una red.

Todo en un momento como el actual, en el que los modelos de seguridad requieren de una verificación de identidad estricta para cada persona y dispositivo (estén dentro o fuera del perímetro) y en el que es más difícil controlar todos los activos (distintos lugares físicos, data-centers o proveedores).

- Favorece el principio del mínimo privilegio: los usuarios sólo acceden a la información y recursos imprescindibles para el desempeño de su actividad.
- Favorece el enfoque Zero Trust: establece un marco de seguridad corporativa en el que sólo usuarios y dispositivos autenticados y autorizados pueden acceder a la información corporativa.
- Ejerce controles de aseguramiento para superficie de ataque: asegura la conexión remota mediante cifrado y los dispositivos de usuario.
- Reduce el riesgo asociado al dispositivo de usuario: permite la evaluación de postura de dispositivos, estableciendo el cumplimiento de los requisitos mínimos de conexión a la hora de acceder a la red.
- Mitiga el riesgo de suplantación de identidad: añade un nivel de seguridad extra mediante doble factor de autenticación (2FA).

3.1.1 Modelo de despliegue

- EMMA ON PREMISE (Hardware/Software):

  Se presenta como *virtual appliance* en el formato de máquina virtual. Se implementa mediante la instalación de una máquina virtual en la infraestructura de la organización (hardware en *appliance* (HW) o software (OVA)).

- EMMA CENTRAL (vSoC).

  Servicio horizontal para que con personal propio y/o subcontratado se concentre el conocimiento y se preste un servicio gestionado de seguridad basado en la capacidad de vigilancia de la infraestructura de red.

Por tanto, la implementación del modelo de Centro Virtual de Operaciones de Ciberseguridad (vSoC) resulta absolutamente imprescindible.

3.1.2 Soporte, instalación y contacto

La solución EMMA será provista como servicio para los Organismos Públicos interesados a través de los Partners de EMMA Certificados (https://www.ccn-cert.cni.es/soluciones-seguridad/emma.html), con soporte telefónico 8x5 y 24x7 a través de correo electrónico (ambos canales en idioma español).