Servicio NGAV (Antivirus de Nueva Generación) y su aportación al cumplimiento del ENS mediante la metodología **µCeENS**

Abstract: *µCeENS es una metodología que posibilita la obtención de una Certificación de Conformidad con el ENS conforme a un Perfil de Cumplimiento Específico (PCE). Para tal fin, µCeENS utiliza una serie de servicios de seguridad proporcionados por herramientas en su modalidad ABS (Análisis Básico de Seguridad), que facilitan la implementación de los requisitos de seguridad asociados.*

Contenido:

1. SOBRE CYTOMIC EPP (NGAV)

NGAV es una solución de seguridad para puestos de usuario y servidores, basada en Cytomic EPP, que está formada por múltiples tecnologías que ofrecen a los clientes un completo servicio de protección contra el malware, sin necesidad de instalar, gestionar o mantener nuevos recursos hardware en la infraestructura de la organización.

Es un software de seguridad muy ligero que se instala en los equipos de la red protegiéndolos de forma centralizada e ininterrumpida, con una única consola de administración web alojada en la nube, accesible en cualquier momento y lugar. La solución NGAV permite además controlar la productividad de los usuarios de la organización, impidiendo el acceso a recursos web sin relación con la actividad de la empresa y filtrando el correo corporativo.

Respecto a la carga de trabajo de los equipos protegidos

Se trata de un software muy ligera al ejecutarse todas las operaciones en la nube, por lo que el impacto en el rendimiento del equipo que lo alberga es prácticamente nulo.

La solución NGAV posee las siguientes características:

- Ligera en consumo de memoria: con un menor tamaño de los ficheros de firmas gracias al acceso en tiempo real a la inteligencia colectiva, que permite desplazar la base de datos de malware del equipo de usuario a la Nube.
- Ligera en consumo de red al reducirse al mínimo el volumen de descargas.
- El fichero de firmas se descarga una vez y se comparte entre todos los equipos de la red.
- Ligera en consumo de procesador al trasladarse la inteligencia de detección a la nube, con lo que se requieren menos recursos de procesador en los equipos protegidos.

Respecto al ámbito de protección de la solución

Al tratarse de una solución multiplataforma cubre la mayoría de vectores de infección en equipos Windows, Linux, macOS y Android, aportando:

- Seguridad en todos los vectores de ataque abarcando la navegación web, el correo electrónico, el sistema de ficheros y el control de los dispositivos conectados al equipo.
- Seguridad, asimismo, contra amenazas desconocidas mediante tecnologías heurísticas y análisis contextuales.

Respecto a la usabilidad de la solución

- Gestión sencilla sin mantenimiento ni necesidad de infraestructuras en la red de la organización.
- Fácil de mantener al no requiere infraestructura específica para alojar la solución.
- Fácil de proteger a los usuarios remotos al comunicarse con la Nube cada uno de los equipos protegidos con independencia de dónde se encuentren; los usuarios desplazados y las delegaciones remotas se protegen de forma transparente, sin requerir instalaciones ni configuraciones VPN particulares.
- Fácil de desplegar al disponer la solución de múltiples métodos para hacerlo, así como con desinstaladores automáticos, que facilitan una rápida migración desde otras soluciones.
- La curva de aprendizaje es muy suave al contar con una interfaz web de gestión intuitiva y sencilla, requiriendo las opciones más utilizadas de un solo clic.

Respecto a la productividad y la seguridad

La solución NGAV monitoriza y filtra el tráfico web y el correo electrónico de forma que la organización pueda centrarse en su área de actividad y competencias sin necesidad de consumir recursos propios para analizar comportamientos inadecuados de sus empleados.

El correo electrónico es una herramienta productiva de carácter crítico en las organizaciones, constituyendo uno de los vectores de ataque más utilizados, lo que exige estar al día en las últimas tecnologías de protección. La navegación por Internet, por otro lado, está expuesta a amenazas tales como los bots, el phishing y el contenido activo malicioso, que comprometen a los usuarios, y por extensión a toda la organización, mientras navegan por Internet.

2. DESCRIPCIÓN DE LA SOLUCIÓN NGAV

NGAV es una solución de seguridad para equipos de usuario y servidores que se basa en la *Inteligencia Colectiva*: una enorme base de datos en la nube, compartida por millones de usuarios, que se alimenta en tiempo real con el conocimiento sobre malware y desinfecciones.

Protección antivirus permanente e Inteligencia Colectiva

En el contexto actual de crecimiento continuo del malware, los servicios alojados en la nube han cobrado especial importancia frente a las actualizaciones del fichero de firmas en forma local. Por esta razón, la protección antimalware de la solución NGAV se basa principalmente en la Inteligencia Colectiva, una plataforma de conocimiento en la Nube que aumenta muy significativamente la capacidad de detección.

Cuando se detecta un nuevo ejemplar de malware en el equipo de un miembro de la comunidad de usuarios, la solución NGAV envía la información a los servidores de Inteligencia Colectiva alojados en la Nube, de forma automática y anónima. Esta información es procesada para generar una solución no sólo para el usuario afectado, sino también para el resto de usuarios de la comunidad, en tiempo real.

Protección con detecciones basadas en contexto

Al margen de la estrategia tradicional de detección, que compara el *payload* del fichero objeto de estudio con el contenido en el fichero de firmas, la solución NGAV implementa varios motores de detección que analizan el comportamiento de los procesos de forma local.

Por ejemplo, a través de la integración con Windows 10 AMSI (AntiMalware Scan Interface) se detectan comportamientos extraños en *scripts* y en las macros embebidas en ficheros ofimáticos.

Además de todo lo anterior, complementariamente, la solución incorpora los tradicionales motores heurísticos y de detección de ficheros maliciosos por características estáticas.

Protección del correo electrónico y la navegación Web

La solución NGAV se aleja del tradicional enfoque de seguridad basado en *plugins* que añaden la funcionalidad de protección a determinados programas (clientes de correo o navegadores). En su lugar, la protección monitoriza a bajo nivel todas las comunicaciones que usan protocolos comunes, tales como HTTP, HTTPS o POP3.

Cortafuegos y sistema de detección de intrusión (IDS)

La solución NGAV supervisa las comunicaciones que recibe o envía cada equipo de la red, bloqueando aquellas que coincidan con las reglas definidas por el administrador. Este módulo es compatible tanto con IPv4 como con IPv6 e incluye varias herramientas para filtrar el tráfico de red:

- Protección mediante cortafuegos basado en reglas que describen las características de una comunicación entre dos (2) equipos: puertos, direcciones IP, protocolos etc. con el objetivo de permitir o denegar los flujos de datos que coincidan con las reglas establecidas.
- Protección de los programas instalados en el equipo de usuario, permitiendo o denegando su comunicación con el resto de la red.
- Protección mediante la detección de intrusiones, detectando y rechazando patrones de tráfico mal conformado que pueda afectar a la seguridad o al rendimiento del equipo protegido.

Control de dispositivos en los equipos

Dispositivos de uso común, tales como las llaves USB, las unidades de CD/DVD, dispositivos de imágenes, bluetooth, módems o teléfonos móviles también pueden constituir una vía de infección para los equipos.

La solución NGAV permite establecer el comportamiento de estos dispositivos en los equipos protegidos, bloqueando su acceso o permitiendo su uso de forma completa o parcial (solo lectura).

Control de acceso a páginas Web

La solución NGAV agrupa las páginas web en varias categorías para que el administrador de la red pueda restringir de un modo eficiente el acceso a aquellas que considere oportunas, así como a aquellas URLs que especifique manualmente. Adicionalmente, permite definir una configuración de horarios para restringir el acceso a determinadas categorías de páginas web y listas negras durante las horas de trabajo y, en su caso, autorizarlo en el horario no laborable.

Parcheo de vulnerabilidades

La solución NGAV mantiene de forma automática una base de datos de los parches y actualizaciones publicadas por los proveedores del software para los sistemas operativos Windows instalados en el parque informático. De esta manera pueden crearse tanto tareas programadas, como inmediatas, para el parcheo de los equipos, reduciendo de esta forma la superficie de exposición de puestos de usuario y servidores.

Visibilidad del estado de la red

La solución NGAV ofrece recursos para valorar el estado de la seguridad de la red en un solo vistazo, a través de los informes y de un panel de control (*dashboard*) formado por diferentes *widgets*. En los paneles se puede encontrar información clave sobre las detecciones realizadas en los diferentes vectores de infección protegidos.

Técnicas de desinfección

En caso de producirse una brecha de seguridad, la solución NGAV revierte los equipos afectados al estado previo a su infección, usando herramientas de desinfección avanzadas y la cuarentena, que almacena los elementos sospechosos o eliminados.

Activación de ficheros de control (Decoy Files)

Al activar la funcionalidad *Decoy Files*, la solución NGAV genera en los equipos ficheros de control que monitoriza de forma permanente. Cuando un proceso modifica estos ficheros, Decoy Files genera una alerta, lo bloquea y lo clasifica como Ransomware (se pueden configurar excepciones).

3. MEDIDAS DE SEGURIDAD EN LAS QUE LA SOLUCIÓN NGAV CONTRIBUYE A µCeENS

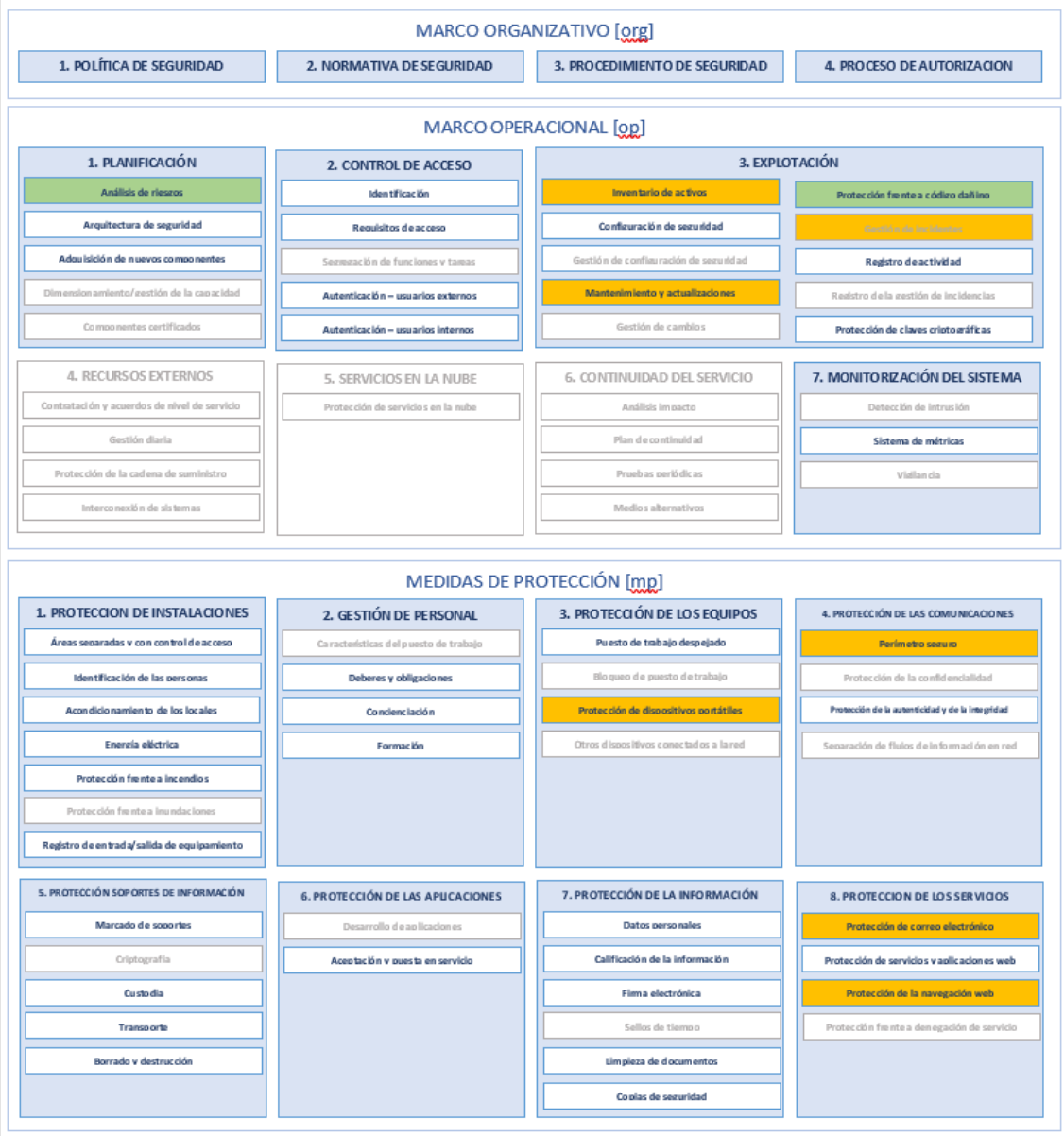
A continuación, se muestran las medidas de seguridad del Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad (PCE-RES) basado en la metodología µCeENS. Se muestran en color gris aquellas medidas del ENS que no intervienen en el PCE-RES.

Dentro de los diferentes grupos de medidas de seguridad, se indican aquellas donde la solución NGAV puede ayudar al cumplimiento en base a dos (2) niveles de contribución: Básico y Medio-Alto.

Considerando que ninguna herramienta garantiza por sí sola el cumplimiento de todas las medidas de seguridad que determina el ENS, la solución NGAV puede ayudar parcialmente al cumplimiento de alguna de ellas.

- **Contribución Básica:** los requisitos abarcan más, aunque la solución NGAV contribuye o ayuda de forma básica al cumplimiento de la medida.

■ **Contribución Media-Alta:** La solución NGAV contribuye de forma media-alta al cumplimiento de la medida.



3.1 LA SOLUCIÓN NGAV EN EL MARCO OPERACIONAL

En el ámbito del marco operacional [op] del Anexo II del ENS cabe destacar las siguientes consideraciones de un enfoque de seguridad centrado en la protección a través de la solución NGAV.

- **PLANIFICACIÓN [op.pl]**
  - **Análisis de Riesgos [op.pl.1]**
    - *La solución dispone de Dashboard e informes que ofrecen toda la información referente a las amenazas detectadas, señalando los activos con más riesgo y las acciones que se han acometido para contener la amenaza.*
    - **Contribución: Media-Alta ■**

- **EXPLOTACIÓN [op.exp]**
  - **Inventario de activos [op.exp.1]**
    - *Se ofrece información de hardware que incluye CPU, memoria, almacenamiento, BIOS y TPM, ofreciendo información relativa al rendimiento de las últimas 24 horas. Incluye información relativa al software instalado, además de incluir un historial de las instalaciones y desinstalaciones que se han realizado.*
    - **Contribución: Básica** ■
  - **Mantenimiento y actualizaciones [op.exp.4]**
    - *La actualización de los sistemas de seguridad es automática, ofreciendo la posibilidad de disponer de las últimas versiones de la solución.*
    - **Contribución: Básica** ■
  - **Protección frente a código dañino [op.exp.6]**
    - *La protección permite la detección de todo tipo de malware, disponiendo de firmas locales, firmas en nube, heurístico, contextual y sistemas anti-ransomware.*
    - **Contribución: Media-Alta** ■
  - **Gestión de incidentes [op.exp.7]**
    - *La solución realiza la contención de los incidentes detectados y comunica por correo electrónico a los contactos indicados. Además, ofrece en la consola la información relacionada con el fin de facilitar la gestión del incidente.*
    - **Contribución: Básica** ■

3.2 CUMPLIMIENTO DE MEDIDAS DE PROTECCIÓN CON LA SOLUCIÓN NGAV

Un enfoque de seguridad centrada en la protección puede ayudar en las siguientes medidas de protección [mp] del Anexo II del ENS:

- **Protección de los equipos [mp.eq]**
  - **Protección de portátiles [mp.eq.3]**
    - *Permite una protección del equipo portátil contra código dañino independientemente de que se encuentre fuera de las instalaciones de la organización. Desde la consola es posible el control del estado de protección del dispositivo portátil.*
    - **Contribución: *Básica*** ■
- **Protección de las comunicaciones [mp.com]**
  - **Perímetro seguro [mp.com.1]**
    - *Con el fin de mejorar la protección perimetral organizativa, se provee de firewall personal en los equipos que permite gestionar los accesos a los equipos y detectar posibles ataques tanto dentro de la organización como fuera.*
    - **Contribución: *Básica*** ■

- **Protección de los servicios [mp.s]**
  - **Protección del correo electrónico (e-mail) [mp.s.1]**
    - *La solución permite la protección del correo electrónico, tanto de su contenido como de sus adjuntos, con interceptación en el transporte POP3 al equipo.*
    - **Contribución:** ***Básica*** ■
  - **Protección de la navegación web [mp.s.3]**
    - *La solución permite la protección de la navegación web, incluyendo un filtro en los protocolos de navegación que monitorizan el contenido de la navegación. Además, dispone de una base de datos de sitios maliciosos para permitir su bloqueo antes de su acceso. Esta protección dispone de servicio anti-phishing.*
    - **Contribución:** ***Básica*** ■

4. CONCLUSIONES

Como se ha comentado, el objetivo de la metodología µCeENS es posibilitar a las entidades en su ámbito de aplicación, una adecuación coherente al ENS y, en consecuencia, la obtención del Certificado de Conformidad con el ENS conforme al Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad.

Análogamente, como hemos mostrado, el propósito de la solución NGAV de Cytomic EPP es proteger a los equipos de ataques de malware, además de ofrecer el control de las actualizaciones de seguridad para el sistema, incluyendo aplicaciones de terceros, reduciendo la superficie de exposición y el riesgo, colaborando así a la adecuación al ENS de los sistemas que la implementan.

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.03.11 00:09:18 +01'00'