CAPÍTULO VII: LA DEFENSA EN PROFUNDIDAD EN SEGURIDAD INFORMÁTICA

Este capítulo tiene como objetivo de conocer los procedimientos de seguridad referente a estaciones de trabajo desde la perspectiva del pentesting y dar las posibles soluciones de los problemas que se detecten al poner a prueba la seguridad de los equipos en la organización, también mostrará la evaluación de las bases de la seguridad de los sistemas y como aprovecharlos para que no puedan afectar a la infraestructura y negocio, también se analiza un punto importante que es la concientización de los usuarios y los riesgos que estos pueden causar a la organización, además de las forma de escribir de forma correcta las contraseñas para minimizar los riesgos de ataques de cibercriminales y evitar el robo de información.

7.1. Tecnología defensiva en seguridad informática

Cuando se habla de tecnología defensiva en el ámbito de la informática, lo primero que se suele venir a la cabeza son los antivirus, pero hay mucha más tecnología que puede complementar la seguridad de lo organización. Lo primero que se debe tener en cuenta es que la responsabilidad de la gestión de la parte tecnológica de la defensa de la infraestructura, ha de recaer sobre el departamento de IT o del centro de operaciones de seguridad, es posible y cada vez más habitual que existan departamentos de seguridad específicos en muchas organizaciones y parte de su labor va a ser coordinado con el trabajo del Departamento de IT, por lo que hay que tener precaución en la gestión administrativa de esta situación.

Cómo se ha analizado en muchas ocasiones, la defensa debe establecerse en profundidad, es decir que se deben aplicar capas de defensa como se muestra en la Figura 105.

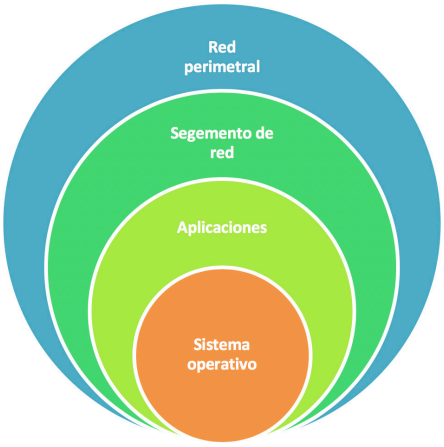

Figura 105. Capas de defensa en profundidad**.**
Fuente: elaboración propia.

Según Rodríguez (2018), indica que cada capa afecta a ciertos recursos y se ocupa de anular o mitigar los riesgos inherentes a dichos recursos, al hablar de soluciones técnicas se está hablando de implementar barreras y de evitar la explotación de

vulnerabilidades. Se puede recorrer esas etapas de seguridad de dentro hacia fuera y ver que soluciones técnicas de seguridad se pueden implementar como se detalla a continuación.

7.1.1. Mantenimiento

En primer lugar, se tiene el propio mantenimiento de los equipos y la aplicación de parches de seguridad, no parece una medida demasiado especial, pero se debe tener en cuenta que si se hace que una vulnerabilidad deje de estar presente en los equipos no se necesitarán poner una capa exterior que impida su explotación.

7.1.2. Antivirus

El siguiente paso sería la instalación de sistemas de antivirus en los servidores y estaciones de trabajo, existen de todo tipo y calidad, unos consumen más y menos recursos, pero hay que contar siempre con ellos y mantenerlos actualizados. Existen los que sólo se basan en firmas, los que emplean sistemas heurísticos, algunos recurren a plataformas online para remitir archivos sospechosos y también hay que hacen sandboxing.

Los antivirus esencialmente son programas que se basan en la detección de malware en la fase de pre- ejecución, es decir que analizan archivos y programas antes de que se ejecuten para prevenir que puedan hacer algo malo. Cada vez está consiguiendo mayor relevancia Windows Defender integrado por la empresa Microsoft en su sistema operativo, no es el más avanzado de los sistemas, pero es bastante eficiente en detección de firmas de malware y además ha mejorado mucho su rendimiento respecto a las primeras versiones, la Figura 106 muestra la pantalla principal de este antivirus.

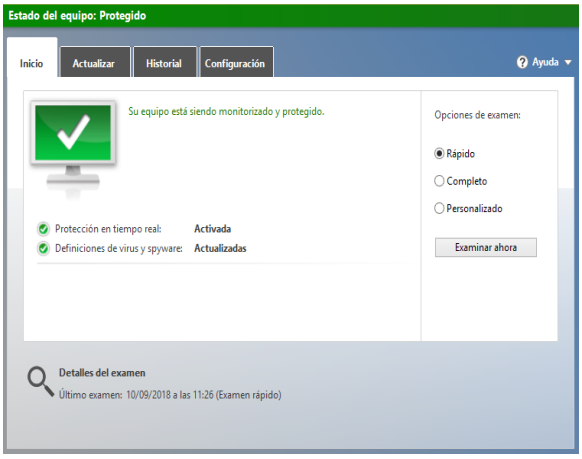

Figura 106. Antivirus Windows Defender.
Fuente: elaboración propia.

Entre las características principales de este antivirus incluye supervisión sobre el estado de configuración del firewall del equipo, sobre la seguridad de las cuentas de usuario e incluso la posibilidad de realizar cierto nivel de monitorización de directorios para protegerlos de ransomware.

7.1.3. EDP y EPP

Los sistemas EDP y EPP siglas de detección y protección en punto final, son cada vez más habituales, en algunos casos se los podría describir como sistemas antimalware que funcionan en modo cliente servidor, es decir, que pueden reportarse a un servidor centralizado que permite tener al administrador visibilidad sobre el estado de seguridad de su infraestructura y recibir alertas sin que el usuario de un equipo tenga que reportarse cuando le salta una ventana de alerta.

Los sistemas EDP y EPP se consideran más avanzados que los tradicionales antivirus por el sistema de gestión centralizado, pero como con cualquier otro producto hay que prestar atención, porque hay algunos que no van más allá que cualquier antivirus y otros bastante más avanzados, entre las principales ventajas de este tipo de sistemas se puede resumir en:

- Son antivirus avanzados
- Añaden detección en ejecución
- Poseen gestión centralizada
- Emiten alertas de incidentes

7.1.4. Firewall software

Ya se ha trabajado desde el propio sistema y desde sus aplicaciones, ahora se va a analizar al estado de red y entre esos puntos está el firewall, todos los sistemas operativos incluyen software de firewall para gestionar sus comunicaciones de red, los hay más y menos desarrollados y también hay varios que se pueden adquirir e instalar en los equipos por el propio usuario.

El objetivo es establecer dos limitaciones, impedir que existan conexiones del exterior hacia el equipo que no sean deseadas, ya que podrían ser ataques o accesos no autorizados y la otra es impedir que existan conexiones salientes desde los equipos porque podrían ser fugas de información gestionadas por ejemplo por un malware que se tenga instalado en el computador.

7.1.5. Seguridad en red

Desde la parte de red se puede implementar medidas de segmentación de redes, proxies de comunicaciones, firewalls, sistemas de detección y prevención de intrusiones, etc., pero eso ya vendrían a formar capas más externas respecto a los servidores y estaciones de trabajo, además no se debe delegar toda la defensa de los equipos a la protección perimetral, porque si se viese superada nada protegería a los equipos, es decir siempre se debe defender a distintos niveles de profundidad como se decía por capas, en resumen en la seguridad de la red se basa en los siguiente puntos:

- Segmentación de redes
- Proxies
- Firewalls
- IDS e IPS