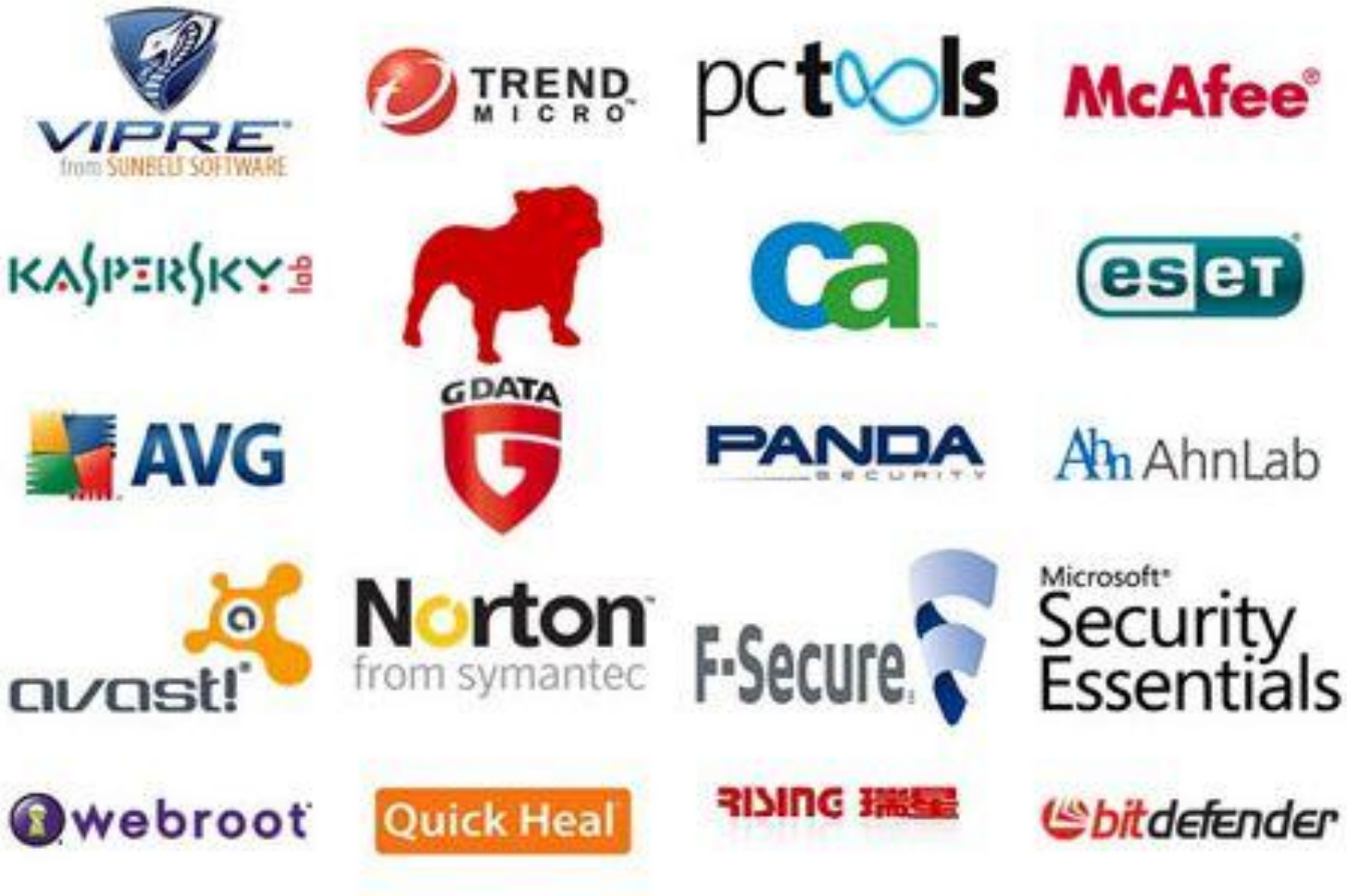
Antivirus

Juan Pablo Parra Pino

Que es el antivirus

- Los **antivirus** son programas cuyo objetivo es detectar y eliminar virus informáticos. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e internet, los antivirus han evolucionado hacia programas más avanzados que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de los mismos. Actualmente son capaces de reconocer otros tipos de *malware* como spyware, gusanos, troyanos, *rootkits*, etc.

METODOS DE FUNCIONAMIENTO



METODOS DE FUNCIONAMIENTO

De acuerdo a la tecnología empleada, un motor de antivirus puede funcionar de diversas formas, pero ninguno es totalmente efectivo, según lo demostrado por Frederick Cohen, quien en 1987 determinó que no existe un algoritmo perfecto para identificar virus.[1]

Algunos de los mecanismos que usan los antivirus para detectar virus son:

- Firma digital: consiste en comparar una marca única del archivo con una base de datos de virus para identificar coincidencias.
- Detección heurística: consiste en el escaneo de los archivos buscando patrones de código que se asemejan a los que se usan en los virus.
- Detección por comportamiento: consiste en escanear el sistema tras detectar un fallo o mal funcionamiento. Por lo general, mediante este mecanismo se pueden detectar software ya identificado o no, pero es una medida que se usa tras la infección.
- Detección por caja de arena (o *sandbox*): consiste en ejecutar el software en máquinas virtuales y determinar si el software ejecuta instrucciones maliciosas o no. A pesar de que este mecanismo es seguro, toma bastante tiempo ejecutar las pruebas antes de ejecutar el software en la máquina real.

Planificación

La planificación consiste en tener preparado un plan de contingencia en caso de que una emergencia de virus se produzca, así como disponer al personal de la formación adecuada para reducir al máximo las acciones que puedan presentar cualquier tipo de riesgo. Cada antivirus puede planear la defensa de una manera, es decir, un antivirus puede hacer un escaneado completo, rápido o de vulnerabilidad según elija el usuario.

Consideraciones de *software*

El *software* es otro de los elementos clave en la parte de planificación. Se debería tener en cuenta la siguiente lista de comprobaciones para tu seguridad:

1. Tener el *software*[2] indispensable para el funcionamiento de la actividad, nunca menos pero tampoco más. Tener controlado al personal en cuanto a la instalación de software es una medida que va implícita. Asimismo, tener controlado el software asegura la calidad de la procedencia del mismo (no debería permitirse *software* pirata o sin garantías). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre.
2. Disponer del *software* de seguridad adecuado. Cada actividad, forma de trabajo y métodos de conexión a Internet requieren una medida diferente de aproximación al problema. En general, las soluciones domésticas, donde únicamente hay un equipo expuesto, no son las mismas que las soluciones empresariales.
3. Métodos de instalación rápidos. Para permitir la reinstalación rápida en caso de contingencia.
4. Asegurar licencias. Determinados *softwares* imponen métodos de instalación de una vez, que dificultan la reinstalación rápida de la red. Dichos programas no siempre tienen alternativas pero ha de buscarse con el fabricante métodos rápidos de instalación.
5. Buscar alternativas más seguras. Existe *software* que es famoso por la cantidad de agujeros de seguridad que introduce. Es imprescindible conocer si se puede encontrar una alternativa que proporcione iguales funcionalidades pero permitiendo una seguridad extra.

Formación del usuario

Esta es la primera barrera de protección de la red.

Antivirus

Es conveniente disponer de una licencia activa de antivirus. Dicha licencia se empleará para la generación de discos de recuperación y emergencia. Sin embargo, no se recomienda en una red el uso continuo de antivirus.

El motivo radica en la cantidad de recursos que dichos programas obtienen del sistema, reduciendo el valor de las inversiones en *hardware*[8] realizadas. Aunque si los recursos son suficientes, este extra de seguridad puede ser muy útil.

Sin embargo, los filtros de correos con detectores de virus son imprescindibles, ya que de esta forma se asegurará una reducción importante de elecciones de usuarios no entrenados que pueden poner en riesgo la red.

Firewalls*Artículo principal:* Cortafuegos (informática)

Filtrar contenidos y puntos de acceso. Eliminar programas que no estén relacionados con la actividad. Tener monitorizado los accesos de los usuarios a la red, permite asimismo reducir la instalación de *software* que no es necesario o que puede generar riesgo para la continuidad del negocio. Su significado es barrera de fuego y no permite que otra persona no autorizada tenga acceso desde otro equipo al tuyo.

Reemplazo de software

Los puntos de entrada en la red la mayoría de las veces son el correo, las páginas web, y la entrada de ficheros desde discos, o de computadoras ajenas a la empresa.

Muchas de estas computadoras emplean programas que pueden ser reemplazados por alternativas más seguras.

Es conveniente llevar un seguimiento de cómo distribuyen bancos, y externos el software, valorar su utilidad.

Centralización y *backup*

La centralización de recursos y garantizar el *backup* de los datos es otra de las pautas fundamentales en la política de seguridad recomendada.

La generación de inventarios de *software*, centralización del mismo y la capacidad de generar instalaciones rápidas proporcionan métodos adicionales de seguridad.

Es importante tener localizado dónde se sitúa la información en la empresa. De esta forma podemos realizar las copias de seguridad de forma adecuada.[9]

Control o separación de la informática móvil, dado que esta está más expuesta a las contingencias de virus.

Empleo de sistemas operativos más seguros

Para servir ficheros no es conveniente disponer de los mismos sistemas operativos que se emplean dentro de las estaciones de trabajo, ya que toda la red en este caso está expuesta a los mismos retos. Una forma de prevenir problemas es disponer de sistemas operativos con arquitecturas diferentes, que permitan garantizar la continuidad de negocio.

Temas acerca de la seguridad

Existen ideas instaladas por parte de las empresas de antivirus parte en la cultura popular que no ayudan a mantener la seguridad de los sistemas de información.

- **Mi sistema no es importante para un cracker.** Este tema se basa en la idea de que no introducir *passwords* seguras en una empresa no entraña riesgos pues «¿Quién va a querer obtener información mía?» Sin embargo, dado que los métodos de contagio se realizan por medio de programas automáticos, desde unas máquinas a otras, estos no distinguen buenos de malos, interesantes de no interesantes. Por tanto abrir sistemas y dejarlos sin claves es facilitar la vida a los virus.
- **Estoy protegido pues no abro archivos que no conozco**. Esto es falso, pues existen múltiples formas de contagio, además los programas realizan acciones sin la supervisión del usuario poniendo en riesgo los sistemas.
- [1]**Como tengo antivirus estoy protegido**. Únicamente estoy protegido mientras el antivirus sepa a lo que se enfrenta y como combatirlo. En general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme las computadoras aumenten las capacidades de comunicación.
- **Como dispongo de un *firewall* no me contagio**. Esto únicamente proporciona una limitada capacidad de respuesta. Las formas de infectarse en una red son múltiples. Unas provienen directamente de accesos a mi sistema (de lo que protege un *firewall*) y otras de conexiones que realizó (de las que no me protege). Emplear usuarios con altos privilegios para realizar conexiones tampoco ayuda.