LabWin 3.x – LabWin, el antivirus y el firewall

Documento finalizado el día: 23/09/2014 – Versión 1.0

Esta nota técnica intenta explicar los distintos puntos a tener en cuenta sobre la configuración del antivirus y el firewall para el uso del sistema LabWin3.

LabWin y el antivirus

Como punto de partida se puede decir que tenemos un componente de LabWin que por su tarea varios antivirus, por heurística, lo detectan como posible amenaza.

El archivo LabWinWS.exe y su tarea

Es el programa encargado de configurar las estaciones de trabajo ya sea cuando se agregan a la red o luego de una actualización del sistema en el servidor. La función de este programa es buscar cualquier componente de LabWin en ejecución a nivel local, terminar el proceso y eliminarlo (en caso de existir) para traer desde el servidor los componentes actualizados y registrarlos (librerías DLL y OCX), agregar las excepciones necesarias al firewall de Windows y por ultimo crear los accesos directos al sistema en el menú Inicio.

Este conjunto de tareas puede que a varios antivirus no les guste y si posee habilitada la función de heurística indique que es una probable variante de algún virus.

Que es la heurística?

Todos los antivirus trabajan con una base de datos de virus conocidos y además poseen esta función que permite evaluar los comportamientos de los programas en busca de acciones “dudosas”. Estas acciones no siempre son virus, e incluso varios antivirus ofrecen la posibilidad de informar falsos positivos.

Uso de protocolos

Cuando un simple programa accede a servicios Web mediante la API del sistema operativo está expuesto a las vulnerabilidades del mismo (algo que a los antivirus no les agrada). Si algún programa utiliza más de dos protocolos de forma exclusiva (HTTP y FTP, por citar ejemplo) para varios antivirus es raro. Otro caso: el programa de envió de informes por mail en laboratorios donde hay muchos pacientes hasta podría interpretarse como un *mail bomber* (el antivirus no analizara la información del mail pero sabrá que el programa está enviando correos a la mansalva).

Configuración personalizada

Lo recomendable es excluir las carpetas del sistema (carpeta LabWin3 del disco local y de la unidad de red) o mejor aun los ejecutables dentro de la misma, ya sea del análisis como del módulo residente del sistema de archivos (en algunos antivirus estas exclusiones se hacen por separado, en distintos apartados de configuración).

Si el volumen de trabajo es alto y la velocidad de la red decae debería evaluar la posibilidad de deshabilitar la heurística. Esta función hace que se revisen las acciones de todos los programas que se ejecutan, por lo que el rendimiento general se ve afectado directamente.

La bóveda o baúl de virus

Cuando el antivirus borra algún ejecutable del sistema se debe restaurar y excluir desde la bóveda o baúl de virus. Algunos antivirus permiten realizar ambas tareas desde la bóveda. En otros será necesario excluir y luego restaurar (si se restaura sin excluir por lo general lo elimina nuevamente al entrar a la carpeta). Durante la instalación del sistema o tareas como la manipulación de una backup previo a formatear el equipo se recomienda trabajar con el antivirus momentáneamente desactivado.

LabWin y el firewall

Conexiones dentro de la LAN

El sistema trabaja en la red local basado en el protocolo NetBIOS (o SMB/CIFS, si así lo prefieren) compartiendo la carpeta en el servidor para conectarla como unidad de red en las terminales. Sobre estos puertos no debería haber problemas, dado que siempre se hayan desbloqueados a nivel de LAN. Para conectar a la base de datos (Firebird) se utiliza el puerto TCP 3050. Si utilizamos algún firewall deberíamos permitir el paso por dicho puerto, siempre dentro de nuestra red local.

Conexiones hacia la WAN

Varios de los módulos adicionales del sistema requieren conexión a servidores externos como es el caso del intercambio de pacientes, donde se suben y descargan ficheros desde nuestro servidor FTP, o el módulo de envió de informes por mail, que requiere conectarse al servidor de correo saliente (SMTP).

De hecho, el protocolo FTP se utiliza bastante, como por ejemplo a la hora de habilitar la licencia (ésta se descarga desde nuestro sitio Web vía FTP) y/o conectar al soporte técnico remoto (mas adelante veremos eso en detalle), por lo que se recomienda que siempre este desbloqueado el puerto 21.

Para el caso de informes por mail se debe permitir el paso hacia el servidor de correo saliente. El puerto estándar es el 25, pero puede variar de acuerdo al proveedor del servicio. En tal caso deberá consultarse la configuración de dicho módulo.

Las autorizaciones on-line (a través del WebService de FABA) se realizan mediante el protocolo HTTP, por lo que no debería haber inconvenientes salvo que dicho protocolo haya sido bloqueado para impedirla navegación en la estación de trabajo.

El programa de soporte técnico remoto

Como disponemos de una dirección IP dinámica, utilizamos un programa que sube a nuestro sitio Web información sobre la dirección IP actual. Al ejecutar el soporte técnico remoto, el equipo del laboratorio lo primero que hace es conectarse vía HTTP a *biodatalab.com.ar* para descargar dicho archivo. Una vez hecho eso levanta el servidor VNC y envía una invitación al cliente (que corre a la espera en nuestros equipos de soporte).

Este es el único medio de conexión que disponemos para brindar soporte remoto ante eventuales problemas y/o dudas sobre el sistema LabWin. Téngalo en cuenta a la hora de aplicar las políticas de seguridad en su red. No utilizamos software como *Team Viewer*. De no poder lograr la conexión vía VNC no podremos hacer mucho desde nuestro departamento de soporte.