INFOSERVICE

Asesoría Impositiva Contable - Peritaje Informático
Procuración – Servicios Especiales

de Miguel Ángel Boldú
CUIT: 20-17879993-3 - IVA Resp. Inscripto
IIBB: 902-128218-3 - Conv. Multilateral

San Juan, 17 de Enero de 2012.-

INFORME PERICIAL PRELIMINAR

EVENTO: Pérdida de Sistema Informático Municipal y Pérdida de archivos de datos críticos

El día 21 de Diciembre de 2011 tomo contacto con el equipamiento informático de la Municipalidad de Zonda (luego de una comunicación telefónica con el Intendente Sr. Cesar Humberto Monla).-

El equipamiento principal consta de un gabinete conteniendo:

1. Un servidor de datos bajo Sistema Operativo Windows Server 2008 Stándard Edition x86 con una aplicación de tipo propietario denominado SIAM de la empresa Proyecto I.
2. Un servidor de aplicación bajo Sistema Operativo Windows XP Professional x86 con la aplicación antivirus PANDA y su licencia para redes.
3. Un servidor externo bajo Linux CentOS Server 4.9 i386 con aplicaciones de uso desconocido para la gestión municipal actual.

Las tareas prioritarias se han enfocado en el Servidor de Datos con Windows Server (en adelante ***Equipo 1***), siguiendo las normativas y procedimientos periciales utilizados por el gabinete Pericial de la Suprema Corte de Justicia de la nación, la División Delitos en Tecnología de la Policía Federal Argentina y normas ISO 27001, las cuales fueron:

a) Revisión de conexionado de router y switch principales.
b) Revisión de arranque del Servidor
c) Revisión de estado de los discos rígidos del Servidor
d) Revisión de Integridad del Sistema Operativo
e) Revisión de los registros de auditoría propios de Windows Server 2008
f) Reconfiguración de las Directivas de Seguridad del Servidor
g) Detección y anulación de aplicaciones “Back Doors” y de control remoto de terminal
h) Revisión y Rescate de archivos borrados pertenecientes al Sistema Operativo, a la aplicación SIAM y archivos varios

a) Revisión de conexionado de router y switch principales.

Se realizó la verificación del cableado estructurado Cat. 5 existente en búsqueda de conexiones clandestinas o no autorizadas, con resultado negativo. Se verificó el router dual D-LINK instalado y se verificó la configuración de conectividad WIFI del mismo, tomándose nota del tráfico ruteado por el equipo.-

b) Revisión de arranque del Servidor.

Mediante el uso de FEDORA 16 i686 Live Security se arrancó el Equipo 1 corriendo diagnósticos de integridad del hardware, encontrándose valores normales y nominales tanto en los parámetros de la motheboard como de la BIOS.

c) Revisión de estado de los discos rígidos del Servidor.

Mediante el uso de las aplicaciones ***gparted***, ***ntfs-3g*** y ***ntfsprogs*** de FEDORA 16 i686 Live Security se corrieron diagnósticos en el disco rígido físico y sus particiones lógicas NTSF. No se hallaron desperfectos mecánicos, eléctricos o lógicos, ni se encontraron fallas en las particiones NTSF. Se encontró una fuerte fragmentación del disco C:, atribuible a la falta de mantenimiento del sistema.-

d) Revisión de Integridad del Sistema Operativo.

Una vez concluida la revisión inicial de hardware se procedió a reiniciar el Equipo 1 y al arranque del Sistema nativo. El mismo se realizó con cierta normalidad, encontrándose pequeñas fallas de acceso de usuario que fueron prontamente rectificadas.-

Una vez iniciada la sesión, se procedió a la revisión de desempeño del Sistema Operativo. Pudo constatarse que había módulos de Windows Server 2008 que fueron desinstalados (Internet Information Services IIS, IPSec, Index Server Service, entre otros). Los mismos son documentados y se reinstalan posteriormente al finalizar el rescate de información.-

Se prosigue con la revisión, encontrando el sistema con parámetros nominales en su desempeño.-

e) Revisión de los registros de auditoría propios de Windows Server 2008.

Se procede a la revisión de los registros de auditoría de seguridad ubicados en la Herramienta Administrativa denominada Visor de Eventos. Allí pueden constatarse registros de ingreso manual al canal ATAPI (es decir el disco rígido) ***con procesos masivos de borrado entre el día 04/12/2011 y el 10/12/2011***. La particularidad de estos registros son:

- Que fueron realizados entre las ***21:00 hs. y las 05:00 hs.*** de esos seis días.
- Que fueron realizados ***en forma remota***, es decir, que el operador no se hallaba físicamente frente al Equipo 1; sino que fue realizado desde una computadora ***externa a la red*** mediante el uso de una aplicación de conexión y control remotos. Los detalles de esta circunstancia serán explicados en un próximo informe.

Los registros fueron asegurados contraescritura y borrado dentro del Servidor y fueron realizadas copias de seguridad de los mismos para ulterior peritaje judicial.-

f) Reconfiguración de las Directivas de Seguridad del Servidor

Habiendo documentado el estado inicial de las Directivas de Seguridad Local –las cuales permitían laxamente el ingreso y manipulación de los archivos sensibles del Sistema Operativo, entre otros- se reconfiguraron las Directivas de Cuenta, Directivas Locales, el Firewall de Windows con seguridad avanzada, Directivas de Restricción de software, Directivas de Control de aplicaciones, Directivas de Seguridad IP en equipo local y la Configuración de Directivas de auditoría avanzada.-

Esto me permite decir que el Servidor se encuentra en condiciones de seguridad operativa normales para ese tipo de equipo.-

g) Detección y anulación de aplicaciones "Back Doors" y de control remoto de terminal.

Se reinició el Equipo 1, arrancando en ambiente FEDORA 16 i686 Live Security para un análisis completo de intrusión y detección de "Back Doors" (Puestas Traseras), troyanos y aplicaciones indeseables que permitan el control remoto del terminal.-

Se utilizaron las aplicaciones ***aide***, ***argus***, ***dsniff***, ***etherape***, ***etercap***, ***hunt***, ***lynis***, ***unhide***, entre otros. Pudo detectarse ingresos a través de los ***puertos 80 (HTPP)*** y ***TCP 5938*** desde la conexión de Internet.-

El tráfico y conexiones entrantes y salientes pueden rastrearse sin problemas cuando son detectadas en el momento. En este caso -al estar desactivados todos los módulos de rastreo automático del Sistema Operativo- solo quedaron rastros de ese tráfico de datos y ordenes. Esos rastros han sido analizados, permitiendo saber cual fue la aplicación responsable de la intrusión.-

Por otra parte, se ha solicitado al proveedor de Internet los registros de tráfico entrantes y salientes desde la antena Canopy Motorola ubicada en la Municipalidad. Con esa información incorporada puede rastrearse el origen de todas las intrusiones y ubicar en forma geográfica al equipo del operador.-

La aplicación responsable de la intrusión se denomina ***TeamViewer***. En la red hay varias terminales (incluido el Equipo 1) que tienen instalado TeamViewer versiones 5 y 6 en forma de ***control remoto*** y con ***control total*** de las computadoras donde están instaladas (este control total permite crear, mover, copiar y borrar cualquier archivo del sistema).Esta aplicación se inicia junto al Sistema Operativo cuando este arranca, por lo que su actividad pasa totalmente desapercibida para un usuario convencional.-

Por cuestiones de seguridad, se anularon todos los puertos que pudieran permitir el control externo del Equipo 1, hasta tanto se restablezca la situación a un estado de normalidad. ***La aplicación fue desactivada***, pero no desinstalada hasta tanto el Equipo 1 vaya a Peritaje Judicial.-

h) Revisión y Rescate de archivos borrados pertenecientes al Sistema Operativo, a la aplicación SIAM y archivos varios.

Una vez asegurado el Equipo 1, se procedió a rescatar la información borrada del Disco C:. Se utilizaron bajo ambiente FEDORA 16 i686 Live Security las aplicaciones ***foremost***, ***hexedit***, ***testdisk***, entre otros.-

Pudieron recuperarse unos 4.7 Gb de información entre archivos de sistema, archivos componentes del sistema SIAM, documentos Word, planillas de cálculo Excel, archivos de imágenes en formato ***jpg*** y ***gif*** (en su mayoría fotos personales y familiares de la antigüa contadora del Municipio) y archivos de video (muchos de ellos con contenido de sexo explícito). Los mismos fueron ubicados en una carpeta de red compartida fuera del disco C: y los clusters (o pistas) ***asegurados contraescritura***, para preservarlas hasta el Peritaje Judicial pertinente.-

Se procedió a hacer un juego de copias de trabajo y un juego de copias de seguridad que quedaron bajo control del Municipio.-

Con las copias de seguridad se procedió a recuperar las bases de datos, índices y módulos del sistema SIAM; mientras que –separadamente- se analizó cada archivo de base de datos (en formato ***dbf***) para recuperar registros marcados para borrado. Los archivos recuperados fueron convertidos en archivos leíbles en Microsoft Access 2010 y cargados en un archivo Access.-

Una copia de los archivos recuperados del sistema SIAM fueron puestos a disposición del Sr. Intendente, para que este los entregara a la empresa Proyecto I para la recuperación de su sistema SIAM.-

Posteriormente mis tareas están consistiendo en el análisis e interpretación de la información rescatada en las bases de datos.-

CALIFICACIÓN LEGAL:

De acuerdo a lo expuesto ut supra, estoy en condiciones de informarle que los hechos acontecidos se encuadrarían dentro de los ***Arts. 153 bis 2º párrafo***, ***157 bis Inc. 1***, del ***Cód. Penal*** en concurso real con los delitos penados por los **Arts. 173 Incs. 8, *11 y 16***, ***174 Incs. 5 y 6***, ***183***, ***184 Incs. 1, 5 y 6***, ***226*** y ***261*** del ***Cód. Penal***; con los agravantes previstos por los ***Arts. 20***, ***20 bis***, ***45***, ***56***, ***210*** y ***277 Inc. 3 punto d)*** del ***Cód. Penal***.-

Esto es por cuanto la intrusión a un sistema público (la red municipal), el borrado de información y el desbaratamiento del sistema administrativo principal del Municipio (lo que ha provocado la inactividad forzosa de muchos servicios públicos municipales con perjuicio directo a la población local) ha sido para encubrir la sistemática sustracción de caudales y bienes públicos por una cifra que –según lo analizado hasta ahora- ronda los ***nueve millones de pesos***.-

Esta aseveración se ve fundada en los registros recuperados hasta el momento; los que permiten rastrear en forma alterna y externa la documentación que intentara hacerse desaparecer para ocultar los delitos cometidos.-

El operador externo que realizó las tareas de borrado debió tener conocimiento interno del sistema al que estaba atacando, sin contar que el mismo debía saber la clave del usuario administrador del Equipo 1. Resulta poco probable que el operador no haya actuado con asistencia de personal y/o funcionarios públicos de esa Repartición Municipal.-

Tampoco es probable inferir la teoría de un atacante solitario, dada la especificidad de los archivos y registros borrados. El operador debía cubrir los rastros de una maniobra ilícita mayor; siendo esta es la conducta típica en los delitos de fraude y sustracción de fondos y bienes registrables.-

Los registros recuperados prueban con un notable grado de certeza ***la participación de*** –cuando menos- ***los funcionarios responsables directos de la confección, firma y pago de los montos sustraídos y de los bienes*** hasta ahora desaparecidos del Municipio.-

Dada su condición de funcionario público con obligación de denuncia, ***le recomiendo*** informar en forma inmediata al Sr. Juez interviniente, aportando las pruebas documentales encontradas y solicitando las medidas periciales pertinentes. En caso de imposibilidad de vuestra parte, puedo realizar tal tarea; dado que actualmente estoy alcanzado por lo establecido en el ***Art. 277 Inc. 1 punto d)*** e ***Inc. 3 puntos a) y d)*** del ***Código Penal*** y el ***Art. 209*** del ***CPPSJ***. A esto se suma la realidad fáctica de estar realizando las tareas propias establecidas en el ***Art. 145*** del ***CPPSJ*** respecto a los consultores técnicos.-

Sobre este punto, solicito a Ud. tenga a bien informar al Asesor Letrado la posibilidad de proponerme ante el Agente Fiscal interviniente en la función de Consultor Técnico; con el objeto de presenciar las operaciones periciales y acompañar en las audiencias como auxiliar y colaborador de esta parte.-

Quedo a vuestra entera disposición y saludo muy Atte.-

Miguel Ángel Boldú
Propietario

Presentado ante la Municipalidad de Zonda
bajo Expte. Nº 0149/2012 el día 19/01/2012