cybex
The Digital Forensic Company
e-newsletter
CYBEX | e-newsletter • Pruebas electrónicas y Computer Forensics
IMPRIMIR SALIR
Septiembre | 2008 | nº 41

Índice

Editorial

Prueba electrónica

Sobre el terreno

Tecnología y procedimientos

Espacio Institucional

Jurisprudencia

Eventos

Pl. Catalunya, 20, 9º · 08002 Barcelona · Tel. 93 272 20 41 Fax. 93 215 50 72
e-newsletter@cybex.es · www.cybex.es • BARCELONA • MADRID • BRUSELAS

JUAN DE LA TORRE
• Grupo Intelligence Bureau

SERGIO AGUD ANDREU
• Cybex

PRUEBAS ELECTRÓNICAS: UNA NUEVA REALIDAD

La irrupción de las nuevas tecnologías y la evolución de los sistemas de información y de telecomunicaciones han aumentado exponencialmente la creación de documentos digitales en las organizaciones.

La creación, distribución y archivo de estos documentos electrónicos, lejos de remitir, se incrementa día a día. Cada año se envían en todo el mundo más de 2,8 trillones de correos electrónicos y, en la actualidad, más del 90% de los documentos que se crean en la organización son ya electrónicos, de los cuales menos del 30% llegan a imprimirse en papel.

Este nuevo entorno digital está cambiando radicalmente el lugar y las estrategias que abogados e investigadores deben seguir para recuperar y presentar estas pruebas tanto en procesos contenciosos como no contenciosos.

Las pruebas tradicionales están migrando desde el papel hacia un entorno virtual, donde los procesos de gestión y criterios de admisibilidad cambian por completo. Además, la Prueba Electrónica está adquiriendo una mayor importancia en los procesos judiciales, exigiendo a todos los actores del ámbito jurídico estas pruebas en sus estrategias legales.

Desde el momento en que se determina la necesidad de adquirir documentos electrónicos, los consultores de Cybex pueden asesorarle sobre la mejor línea a seguir para salvaguardar y adquirir las pruebas disponibles, así como el tiempo y los costes asociados.

Al utilizar de forma anticipada los servicios de los consultores de Prueba Electrónica, además de maximizar la posibilidad de obtener documentos pertinentes en un primer análisis, éstos pueden detectar posibles oportunidades y ventajas antes de iniciar cualquier proceso.

Aprovechamos la ocasión para enviarle un cordial saludo.

MANUEL BELLIDO ASPAS
• Magistrado de lo Social

EL PODER DE CONTROL DEL EMPRESARIO SOBRE LOS NUEVOS MEDIOS DE COMUNICACIÓN E INFORMACIÓN EN LA EMPRESA Y SUS LÍMITES (II)

LÍMITES DEL CONTROL EMPRESARIAL

Como ya se ha señalado al comienzo de este artículo, uno de los principales problemas para delimitar el control empresarial de los medios informáticos de comunicación e información viene determinado por la escasa regulación legal existente. Así, los únicos preceptos del Estatuto de los Trabajadores que conforman el marco legal básico de la materia tratada son el art. 20.3, en virtud del cual "*el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso*". Y el apartado a) del art. 5 del mismo Cuerpo Legal que, con carácter muy general, impone a los trabajadores como uno de sus deberes básicos el de "*cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad a las reglas de la buena fe y diligencia*".

Como puede verse, se trata de una regulación general, no pensada para resolver los problemas específicos que pueden plantearse en el ámbito de las nuevas tecnologías, consecuente con la fecha de redacción de la norma estatutaria, en la que no se habían generalizado los problemas actuales. Por otra parte, es menester reconocer que los avances tecnológicos siempre van por delante de las leyes, y resulta difícil establecer marcos legales estables sobre materias que evolucionan muy rápidamente. Sin embargo, sería deseable una regulación legal más detallada, al menos sobre los aspectos básicos del uso de los instrumentos informáticos y de los límites del control empresarial.

Con todo, tal vez la vía más adecuada para regular esta materia venga de la mano de la negociación colectiva. Son los convenios colectivos, en particular los de empresa, el marco legal más adecuado para regular los usos permitidos y prohibidos, así como las consecuencias disciplinarias del incumplimiento y los medios de control y fiscalización a establecer por el empresario. Esta

regulación convencional permite a las partes negociadoras adecuarse a las características concretas de cada empresa: su tamaño y capacidad económica, el sector de actividad y desarrollo tecnológico, etc. En todo caso, esta regulación debe sujetarse a dos premisas básicas: de una parte, el legítimo derecho del empresario a controlar el adecuado uso de las herramientas y medios técnicos, de otra, la necesaria salvaguarda de los derechos a la intimidad y al secreto de las comunicaciones de los trabajadores y a su dignidad humana.

Sentado lo anterior, procede entrar a conocer límites que debe respetar el empresario en el control de los medios informáticos.

1. Control empresarial conforme a la buena fe

En la prestación derivada del contrato de trabajo, no sólo es el trabajador el que está sujeto a cumplir con las obligaciones propias de su puesto de trabajo de conformidad con las reglas de la buena fe y diligencia, también el empresario debe ejercer su poder de dirección y control respetando los mismos principios. Así lo establece el art. 20.2 del Estatuto de los Trabajadores al disponer que "*el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe*".

Esta exigencia de buena fe en el control empresarial requiere, como ya se ha adelantado al tratar el derecho a la intimidad, que los trabajadores tengan conocimiento de las condiciones de uso de las herramientas informáticas y, en particular, de las actuaciones que les están prohibidas. También de la posibilidad de que el uso del ordenador sea objeto de control y fiscalización por parte del empresario, de tal manera que los controles no constituyan una sorpresa para el trabajador, que puede haber venido actuando en la creencia de que el uso particular del correo electrónico o de la navegación por internet era aceptado por la empresa o, al menos, no estaba sujeto a control alguno[1], de tal manera que un control sorpresivo constituiría una intromisión inaceptable en la intimidad del trabajador.

Este conocimiento de las condiciones de uso del correo electrónico e internet, así como de los controles a que están sujetos, se consigue estableciendo códigos de conducta, normalmente incluidos dentro de los convenios colectivos, pero que también pueden incorporarse al contrato de trabajo mediante un anexo. Otra posibilidad es la de darles la suficiente publicidad dentro de la empresa (tablón de anuncios, entrega de una circular a los trabajadores, etc.). Con los actuales medios técnicos, incluso resulta posible que los programas informáticos instalados avisen al

[1] Así se recoge en la sentencia del TSJ de la Comunidad Valenciana de 19-07-05 (AS 2005/3205).

trabajador de las actuaciones prohibidas al hacer uso de ellos.
En lo que respecta a las condiciones de uso, lo normal es que la empresa autorice un uso amplio y general del correo electrónico para usos profesionales, con la obligación excepcional de obtener autorización para usos, también profesionales, que excedan de los habituales y puedan generar algún riesgo para la empresa (Vg., envíos masivos o de especial complejidad). De contrario, se suele prohibir el uso del correo electrónico o la navegación por internet con una finalidad privada, si bien esta prohibición general se refiere, fundamentalmente, a un uso abusivo, tolerándose en muchos casos un uso privado moderado por la vía de identificar y detallar tan solo conductas concretas que están terminantemente prohibidas, ya sea por su carácter ilegal u ofensivo (falsificación de mensajes, envío de material ofensivo, inapropiado, con contenidos discriminatorios o que promuevan el acoso sexual o moral o inciten a la violencia, etc.) o por perjudicar directamente la organización o funcionamiento de la empresa (envíos correos masivos, con archivos anexos de gran tamaño, que interfieran o colapsen las comunicaciones, etc.)[2].

También se detallan en los convenios colectivos las faltas que pueden cometerse mediante el uso de estas herramientas informáticas y las correspondientes sanciones.

Como ya se adelantó al tratar de los derechos fundamentales que es necesario respetar en el control empresarial de las herramientas informáticas, el conocimiento por el trabajador de los usos permitidos y prohibidos y de la posible fiscalización o auditoria de los ordenadores, impide que el trabajador vulnerador de las instrucciones empresariales pueda escudarse en la existencia de una "*expectativa razonable de intimidad*" digna de protección, dado que es perfecto conocedor de que la utilización privada y abusiva que realiza del correo electrónico o internet, mediante la utilización de medios de producción de la empresa, está prohibida y puede ser controlada.

2. Control empresarial razonable y justificado

La generalización del uso del correo electrónico e internet en todos los ámbitos, incluido el laboral, genera en los trabajadores una expectativa de confidencialidad, al menos cuando el uso privado que realizan no es abusivo o ilegal, de tal manera que el control empresarial tampoco puede ser abusivo ni arbitrario. Dados los derechos fundamentales en juego -intimidad y secreto de las comuniciones-, parece lógico exigir que el control o registro de los ordenadores obedezca a la existencia de indicios o sospechas de un uso indebido[3].

[2] Un ejemplo de este tipo de regulación, utilizando el convenio colectivo, es el de la empresa Telefónica de España SAU para los años 2003/2005, cláusula 21.5 (BOE de 16-10-03).

[3] Así lo entiende, entre otras, las sentencias de los TSJ de la Comunidad Valenciana de 19-07-05 (AS 2005/1343) y Cantabria, de 26-08-04 (AS 2004/2513).

Con todo, no cabe descartar un control genérico o aleatorio si el mismo es conocido por los trabajadores y está justificado por la necesidad de verificar el correcto funcionamiento de los sistemas informáticos de la empresa o la adecuada prestación de servicios, especialmente en el caso de empresas que atienden a sus clientes o prestan servicios a través del correo electrónico o internet. Así lo ha admitido nuestro Tribunal Supremo para las empresas de tele marketing telefónico[4].

3. Control empresarial necesario y proporcionado

En el caso del control empresarial de los medios de comunicación e información, como en todos aquellos en los que se produce una colisión entre derechos, resulta imprescindible que las medidas que se adopten, en cuanto restringen derechos fundamentales, superen el juicio constitucional de proporcionalidad[5].

Conforme al mismo resulta necesario que la actuación limitadora cumpla tres requisitos:

a) Que sea susceptible de conseguir el objetivo propuesto (juicio de idoneidad).
b) Que resulte necesaria, de tal manera que no exista otra menos limitativa del derecho que permita conseguir los mismos fines (juicio de necesidad).
c) Que la misma sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

Como ha señalado el Tribunal Constitucional en múltiples sentencias, en particular en supuestos similares como los relativos a la instalación de sistemas de video vigilancia, las resoluciones judiciales que conozcan de estos supuestos deben proceder a una ponderación adecuada, que respete la correcta definición y valoración constitucional del derecho fundamental en juego y de las obligaciones laborales que pueden modularlo. "*Estas limitaciones o modulaciones tienen que ser las indispensables y estrictamente necesarias para satisfacer un interés empresarial merecedor de tutela y protección, de manera que si existen otras posibilidades de satisfacer dicho interés menos agresivas y afectantes del derecho en cuestión, habrá que emplear estas últimas y no aquellas otras más agresivas y afectantes. Se trata, en definitiva, de la aplicación del principio de proporcionalidad*" [6].

[4] STS de 5-12-03 (RJ 2004/313), a la que ya se ha hecho referencia en la nota 1 al pie de página.
[5] A él se refieren las SSTC 186/2000, 37/1998 ó 207/1996. También ha sido recogido por sentencias laborales como las dictadas por el TSJ de Cataluña de 22-07-04 (EDJ 2004/93282) y el TSJ de Madrid, de 13-05-03 (AS 2003/3649).
[6] SSTC 98/2000, de 10 de abril y 186/2000, de 10 de julio ya mencionadas en la nota 5.

Ante la existencia de indicios de que un trabajador está efectuando un uso indebido del correo electrónico, el empresario deberá valorar las circunstancias concurrentes, tales como las sospechas o indicios de uso indebido existentes, la posible gravedad de las conductas y los perjuicios que pueden derivarse para la empresa, entre otras, adoptando aquellos medios de control menos lesivos para los derechos del trabajador que permitan conseguir el fin propuesto. Por su parte, el órgano judicial que, en su caso, pueda conocer de la demanda interpuesta por el trabajador, también deberá valorar todas las circunstancias concurrentes: el fin perseguido con la instalación de mecanismos de control, su justificación, el conocimiento por parte de los trabajadores, la actividad a la que se dedica la empresa, etc., al objeto de determinar si se ha producido una vulneración del derecho fundamental.

Dentro de los programas de control del uso del correo electrónico que pueda instalar el empresario, serán preferibles aquellos dirigidos a discriminar el carácter profesional o privado de los mensajes enviados, el número de estos, los destinatarios, el tiempo dedicado a la actividad, etc., dejando para aquellos supuestos en los que resulte estrictamente necesario y sea admisible, el posible control del contenido de los mensajes.

4. Control empresarial sujeto a un procedimiento que garantice los derechos del trabajador y que respete su dignidad como persona

Por último, el control de las comunicaciones informáticas debe someterse a procedimientos que permitan la máxima transparencia y eviten la indefensión del trabajador, respetando su dignidad. Al respecto, diversas resoluciones judiciales de las Salas de lo Social de los Tribunales Superiores de Justicia[7] venían exigiendo la aplicación analógica del procedimiento previsto en el art. 18 ET para el registro de las taquillas y efectos particulares del empleado, esto es: presencia de un representante de los trabajadores, en horario legal y con respeto a la dignidad e intimidad del trabajador.

La extensión de este precepto al registro de los ordenadores resulta problemática, por cuanto se trata de medios de producción de la empresa, de manera que el empresario tiene derecho a verificar en los ordenadores el correcto cumplimiento de la prestación de trabajo. Por el contrario, las taquillas son espacios exclusivamente personales de los trabajadores cedidos por la empresa, de manera que, aun cuando esta cesión está vinculada al contrato de trabajo, queda al margen

[7] Sentencias del TSJ de Cantabria de 26 de agosto y 20 de febrero de 2004 (AS 2004/2513; EDJ 2004/44109, respectivamente); sentencia del TSJ de Cataluña de 22 de julio de 2004 (EDJ 2004/93282); sentencia del TSJ de Andalucía (Málaga), de 25 de febrero de 2000 (AS 2000/562).

de su ejecución y de los poderes empresariales del art. 20 ET.

Esta importante diferencia ha llevado a que otras sentencias[8] hayan considerado que el carácter de medios de propiedad empresarial que tienen los ordenadores no permite atribuirles el ámbito de privacidad que, por el contrario, sí tienen las taquillas y otros espacios personales de los empleados, de manera que su control no requiere sujetarse a los requisitos del art. 18 ET.

La cuestión ha sido resuelta por la sentencia ya comentada del TS de 26-09-07, que no considera aplicable a estos supuestos los límites y garantías previstos en el art. 18 ET. En síntesis, las razones expuestas por el Alto Tribunal son:

1ª. El registro de las taquillas o efectos personales del trabajador excede del poder de dirección y control de la actividad laboral que otorga al empresario el art. 20.3 ET, y se justifica en la necesidad de proteger el patrimonio empresarial y de los demás trabajadores. Sin embargo, tratándose de los ordenadores de la empresa, la legitimidad del control deriva de su carácter de instrumento de producción, de manera que el empresario debe controlar su uso para verificar si se ajusta a las actividades laborales de la empresa. También debe verificar los contenidos y resultados de la prestación[9]. Existen además otros motivos genéricos que justifican el control empresarial: coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencia de los trabajadores (pedidos, relaciones con los clientes...), protección del sistema informático de la empresa que puede verse afectado por determinados usos, prevención de responsabilidades empresariales por usos indebidos o ilícitos, etc.

2ª. Los requisitos o garantías del proceso de registro exigidos por el art. 18 ET: que el registro se practique en el centro de trabajo y en horas de trabajo, y en presencia de un representante legal de los trabajadores o, en su defecto, de otro trabajador de la empresa, no deben ponerse en relación con la protección de la intimidad del trabajador, sino considerarse limitaciones que hacen menos gravosa la posibilidad excepcional de que el empresario pueda registrar al trabajador, o sus objetos personales y taquillas, así como garantías de la objetividad y eficacia de la prueba,

[8] Entre otras las sentencias del TSJ de Madrid, de 13 de noviembre de 2001 (AS 2002/471) y del TSJ de Cataluña de 5 de julio de 2000 (AS 2000/3452).

[9] La STS 26-09-07 menciona la de la misma Sala de 5-12-03, sobre tele marketing telefónico, que aceptó la legalidad del control empresarial consistente en la audición y grabación aleatorias de las conversaciones telefónicas entre los trabajadores y clientes para corregir los defectos de técnica comercial, a la que se ha hecho referencia.

como establece también el art. 569 LECRM para intervenciones similares.
Por tanto, estas garantías no tienen sentido en el control normal de los medios de producción de la empresa[10]. Cuestión distinta es que, aun no siendo necesarias para la validez del control, resulten convenientes para asegurar la prueba obtenida y despejar cualquier duda acerca de su posible manipulación, tanto en la obtención como en la posterior custodia hasta la presentación ante el órgano judicial. Así, en el momento de proceder al registro del ordenador lo más correcto es que esté presente un representante legal de los trabajadores y el propio afectado. También puede efectuarse en presencia de un fedatario público como es el notario. Igualmente el depósito y custodia de la información obtenida -normalmente el disco duro del ordenador- deberá garantizar su integridad, por lo que normalmente se deposita ante notario, obteniéndose una copia idéntica para aportarla en juicio, de tal manera que siempre existe la posibilidad de una contraprueba pericial, confrontándola con el original no manipulado.

CONSECUENCIAS DE USO INDEBIDO POR EL TRABAJADOR DE LOS MEDIOS INFORMÁTICOS DE COMUNICACIÓN E INFORMACIÓN

Las consecuencias de la utilización indebida por el trabajador del correo electrónico e internet pueden dar lugar a su responsabilidad disciplinaria, que abarcará desde una sanción hasta el despido disciplinario. Para ello será necesario que la conducta del trabajador pueda encuadrarse dentro de alguno de los incumplimientos contractuales previstos en el art. 54.2 ET y que reúna las notas de gravedad y culpabilidad.

Aunque la casuística de nuestros tribunales es muy variada, el motivo de despido más alegado por el empresario es la trasgresión de la buena fe contractual, así como el abuso de confianza en el desempeño del trabajo (art. 54.2.d) ET), por ser el de más fácil acreditación, incluyéndose dentro de este apartado múltiples supuestos. Sin embargo, en ocasiones también se ha alegado la desobediencia a las órdenes empresariales (art. 54.2.b) ET), en aquellos casos en los que el trabajador efectúa un uso del correo electrónico o internet expresamente prohibido por el empresario[11] e, incluso, podría pensarse en la alegación de la causa prevista en la letra e) del mismo precepto, la disminución continuada y voluntaria en el rendimiento de trabajo normal o pactado, para aquellos supuestos en los que el trabajador se dedica a navegar por internet o a enviar y recibir correos electrónicos privados en horas de trabajo.

[10] La STS 26-09-07 también hace referencia a la ausencia del trabajador afectado en el registro del ordenador, dado que la sentencia del Juzgado de lo Social que dio lugar al recurso la considera como atentatoria contra la dignidad de propio trabajador. La sentencia del Tribunal Supremo entiende que la presencia del trabajador en el registro, exigida por el art. 18 ET, pero también por el art. 20.3 ET y, en general, consustancial a todas las formas de control empresarial, no puede vincularse con el respeto a la dignidad humana. Que el trabajador no esté presente en el control no puede considerarse que atente contra su dignidad.

[11] STSJ de Cataluña de 5-07-00 (AS 2000/3452).

Con todo, como ya se ha insistido a lo largo de este trabajo, existe un uso privado moderado de estos medios de comunicación e información que está socialmente aceptado. Por ello, y por la aplicación por nuestra jurisprudencia social de la teoría gradualista en el despido, que exige, al valorar la legitimidad de la máxima sanción laboral, la existencia de proporción entre las circunstancias del hecho y del autor y la sanción a imponer, no bastará normalmente con la mera utilización privada de estos medios informáticos para justificar el despido, sino que será necesario que la conducta del trabajador revista gravedad suficiente. En este sentido y, a salvo de la concurrencia de otras circunstancias que evidencien la gravedad, se debe exigir un uso abusivo que exceda del simple uso excepcional. Todo ello sin perjuicio de que se pueda imponer otra sanción distinta al despido en aquellos supuestos en que la conducta del trabajador no alcance la necesaria gravedad. Esta sanción deberá estar suficientemente tipificada.

CONCLUSIÓN

La utilización de las nuevas tecnologías de la comunicación en el ámbito laboral abre un importante abanico de posibilidades, con grandes ventajas tanto para las empresas como para los trabajadores, aunque no está exenta de dificultades y problemas que deberán ir solucionándose conforme se planteen, atendiendo a dos premisas básicas a las que ya se ha hecho referencia: el legítimo control del empresario sobre los medios de producción de la empresa y el contenido de la prestación laboral, y el respeto de los derechos de los trabajadores.

Aun cuando la rapidez de los avances tecnológicos dificulta una regulación legal estable, el ordenamiento laboral cuenta con la ventaja de la negociación colectiva, que permite regular las condiciones de uso de las herramientas informáticas y los medios de control empresarial, adecuándolos al estado de la técnica informática. Son los convenios colectivos los que están llamados a regular en el futuro los códigos de conducta a seguir en el uso de las herramientas informáticas.

Hasta que estos códigos de conducta se generalicen habrá que estar a la escasa regulación legal existente y a la interpretación que de la misma se hace por los tribunales sociales, en particular por la jurisprudencia del Tribunal Supremo, buscando el siempre difícil equilibrio entre los intereses y derechos contrapuestos que entran en juego.

Nota: Este trabajo de Manuel Bellido Aspas se publica por capítulos en los Newsletters de Cybex de Julio/Agosto y Septiembre.

NORMAN HOPPÉ

• Experto en Gestión de Riesgos de la Información · ING Group, Amsterdam

LA PROTECCIÓN DE LAS GRANDES ORGANIZACIONES FRENTE AL DELITO ELECTRÓNICO

Cuando usamos la expresión "delito electrónico" se nos ocurren varios tipos de actividades indeseables, entre ellas el uso de software malicioso, como virus, gusanos y troyanos. Sin embargo, incluso teniendo en cuenta la ultima generación de 'súper-troyanos', esto es sólo una pequeña parte del 'todo', que es definido de manera diferente por organizaciones diferentes. No obstante, la definición que sigue es una combinación de las dos definiciones mas comúnmente aceptadas:

"el delito electrónico es cualquier crimen cometido mediante el uso de un aparato electrónico o interfaz o programa informático – o que haya sido perpetrado contra alguno de estos, o todos ellos"

Ciertamente, esta definición es muy amplia – y, en cualquier caso, ¿por qué deberían importarnos las definiciones?– La respuesta es que en una organización comercial o un departamento gubernamental es necesario dedicar recursos materiales y humanos a la lucha contra este tipo de delitos, al igual que a otros riesgos relacionados con la información y los sistemas informáticos. Sólo una vez que entendamos la magnitud de aquello contra lo que estamos luchando podremos reclutar y capacitar personal, así como establecer actividades y mecanismos de control, estructuras para medir e informar sobre la vulnerabilidad, y la autoridad necesaria para hacerle frente.

Hace quince o veinte años, los programas maliciosos y los ataques externos representaban alrededor del quince por ciento del total del riesgo criminal en nuestra área, según datos del FBI y diferentes encuestas. Hoy en día, naturalmente, ese porcentaje es mucho más alto, con Internet en pleno apogeo y el comercio electrónico como elemento esencial de muchos modelos de negocio. No obstante, estableciendo un conjunto adecuado de controles técnicos, la vulnerabilidad debería ser limitada, al menos operacionalmente.

Jerome Kerviel, de Societée General, y antes de él Nick Leeson, de Barings (precedidos por un conjunto pequeño pero significativo de corredores de bolsa irresponsables y pertenecientes a algunas

de las principales instituciones financieras del mundo) no habrían sido mas que corredores de bolsa normales y totalmente anónimos, si no hubieran escapado a ciertos controles básicos de acceso y de segregación de responsabilidades; o si sus compañías hubieran aplicado las medidas de control de procesos que actualmente son exigidas por ley y por diversos reglamentos en todo el mundo.

He investigado casos de sabotaje de sistemas informáticos, amenazas criminales, uso inapropiado de sistemas, pedofilia, pornografía y, por supuesto, dos o tres modalidades de fraude informático. Esto es el lado 'fuerte' del delito electrónico, en el que las consecuencias no se limitan a pérdidas financieras directas, sino que a menudo conllevan importantes daños a la reputación y a la cuota de mercado, mucho más graves que las pérdidas directas. Sin embargo, muchos de estos delitos fueron cometidos de forma oportunista; es decir, los 'delincuentes' se aprovecharon de mecanismos débiles o de un entorno de débil disciplina y baja calidad. A menudo, los mismos 'delincuentes' iniciaron los actos delictivos como un juego o una venganza que se les fue de las manos.

El primer gran 'fraude', que además está muy bien documentado, nunca llegó a juicio debido a que en aquellos tiempos era demasiado difícil llevar este tipo de casos a los tribunales. A principios de los setenta, dos programadores del Centro Informático de la Oficina Tributaria estadounidense redondearon todos los puntos decimales en cada declaración de impuestos y transfirieron el excedente a sus propias cuentas bancarias. Teniendo en cuenta el gran número de contribuyentes, estas cantidades ínfimas pronto sumaron muchos miles de dólares. Nadie pudo identificar un crimen, ni tampoco una víctima individual que estuviera dispuesta a iniciar un proceso legal, o fuera capaz de correr con los gastos. Los delincuentes emigraron a Suiza y ganaron mucho más dinero escribiendo sobre su 'juego' y, posteriormente, ganaron aun más como consultores expertos en el combate contra el delito electrónico.

Por otro lado, está el ciber-terrorismo. Si algo necesita ser definido, es este concepto. En los años setenta se acusó a Black September de robar las copias de seguridad de una de las más importantes compañías automovilísticas de Europa y provocar la caída sus sistemas principales, para finalmente conseguir mediante chantaje la entrega de dinero a cambio de las copias. Desde entonces, a pesar de los chismes e insinuaciones al respecto, no existe constancia pública de ningún ataque 'terrorista' a sistemas o mediante el uso de sistemas.

En los noventa, se nos bombardeaba constantemente con la amenaza del ciber-terrorismo, y ese 'bombardeo' provenía de los propios servicios de seguridad, que en ese momento – tras el colapso de la Unión Soviética – estaban necesitados de nuevos roles y financiación. Hoy en día, no están faltos de trabajo, y esa amenaza ya no se escucha tanto.

El más reciente – y peor – ejemplo de este tipo de exageración es un documental de la BBC que recibió mucha atención mediática y que simplemente mostraba a un terrorista usando Internet como medio de comunicación (al igual que el resto de las malas – y buenas – personas del mundo).

He aquí, pues, la necesidad de atajar toda esta maldad generada por ordenadores, en parte real y en parte no tanto, junto con los riesgos 'normales' a los que se enfrentan los sistemas informáticos, que incluyen la calidad, adquisición, externalización y, naturalmente, la gestión de la continuidad. Ahora probablemente se vea con más claridad que las definiciones son necesarias para proceder con la estructuración de los tres conjuntos de controles básicos para la mitigación de riesgos: Organización, Métodos y Sistemas.

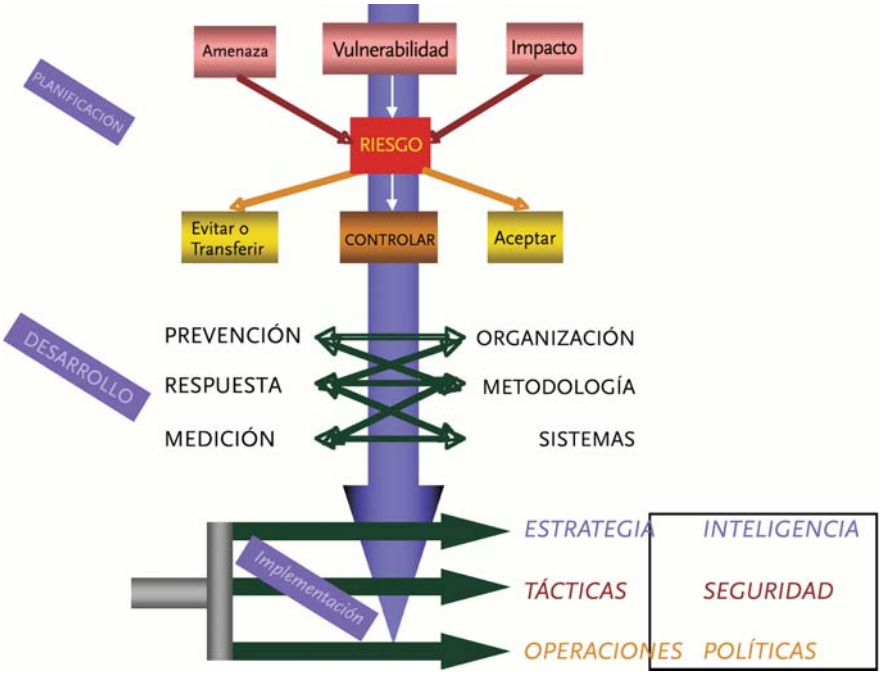
Evidentemente, hoy en día no existe en el mundo ninguna gran organización que no tenga absolutamente ninguna función responsable de la gestión de riesgos y sus derivados, desde la gestión de riesgos no financieros hasta la gestión de riesgos de la información, la gestión de riesgos informáticos y la seguridad de los sistemas informáticos, y que maneje estos elementos a nivel estratégico, táctico y operacional (las tres líneas de defensa).

No obstante, es otra cuestión muy diferente si esas organizaciones pueden con la mano en el corazón decir que cuentan con todos los componentes y que todos ellos funcionan en armonía como un todo, protegiendo a la organización de los riesgos **actuales** y ofreciendo a la Junta información precisa sobre el nivel de riesgo.

Pienso que es posible reducir todas las cuestiones a grupos de tres, y después trabajar sobre ellas en una forma razonablemente lógica, que pueda ser implementada y resulte útil.

El siguiente diagrama de flujo a (muy) alto nivel ilustra el enfoque que desarrollé en 1987, y al cual llamé Metodología Trident.

La protección de la información: Diagrama de flujo en formato Trident



Esta metodología se denomina Trident debido a que todo en el entorno de protección de la información se organiza, de manera más o menos natural, en grupos de tres elementos. Esto permite adoptar la vieja filosofía de dividir las cuestiones de gran complejidad en partes que se puedan manejar de forma lógica.

La **"planificación"** se basa en la Evaluación de Riesgos, que a su vez debería ofrecer los medios para gestionar el riesgo (aceptación, evasión, o transferencia y control). El diagrama muestra el flujo de actividad a muy alto nivel, y además existen varios otros diagramas más detallados y descripciones a niveles más bajos que refuerzan cada uno de los elementos del diagrama mostrado arriba.

El **"desarrollo"** ha de ser un programa complejo, como indica sutilmente la matriz de alto nivel.

La **"implementación"** siempre va a resultar la parte más difícil, y esta dificultad reside en la transición desde la aceptación del plan por parte de la Junta Directiva a la instalación de mecanismos de control de cualquier tipo (es decir: lograr cambios). Siempre me sorprende cómo, cuando se

intentan implementar enfoques basados en los controles internos, existen programas definidos y excelentes soluciones externas previamente aceptadas por la Junta y que además poseen recursos y presupuestos, pero aún con todo esto, nunca se llegan a implementar totalmente. Incluso cuando algunos mecanismos de control son finalmente 'instalados', a veces son ignorados o pasados por alto en el entorno operativo. Si bien hay formas de evitar estas dificultades, su descripción probablemente ameritaría otro artículo.

Quisiera basarme en el diagrama 'Trident' (arriba) para ir más lejos. Es posible desglosarlo desde cualquier punto, pero dado que estoy discutiendo el desarrollo de una herramienta para hacer frente al delito electrónico, me parece que lo mas adecuado es describir el enfoque desde el punto de vista de la Organización, Metodología y Sistemas/Tecnología.

Antes de profundizar más, es necesario aclarar un punto importante: Hoy en día, cualquier organización que desee realmente gestionar sus riesgos de la información ha de invertir en herramientas tecnológicas y contratar los servicios de especialistas externos, no sólo para cuestiones tradicionales como la gestión del control de acceso y la protección criptográfica, sino además para la gestión de la información/conocimiento, la evaluación de riesgos, la vigilancia e informes del cumplimiento normativo y, por supuesto, el análisis forense.

Dicha organización deberá contratar los servicios de profesionales externos en el área de respuesta (investigación, análisis de incidentes, etc.) y probablemente también en algunas áreas relacionadas con el desarrollo de medidas preventivas complejas.

El uso de la tecnología y los servicios sugerido en los párrafos precedentes facilita la gestión de riesgos de la información de forma rentable. En el mejor de los casos, si se ignoran dichas sugerencias en una compañía moderna por encima del nivel PYME, solo se podrá desarrollar un enfoque esporádico y limitado. Posiblemente se proveerán los medios necesarios para la auto-evaluación y el control en las líneas de negocio (con la esperanza de que aquellas funciones del negocio que deberían ser controladas objetivamente, se auto-controlarán de manera voluntaria, informando de las malas noticias además de las buenas). Intentar cubrirlo todo sin herramientas tecnológicas y sin los servicios de especialistas externos siempre resultará demasiados costoso como para ser rentable, comparado con una visión pragmática del valor de aquello que se está intentando proteger, la probabilidad y la potencial frecuencia de los ataques.

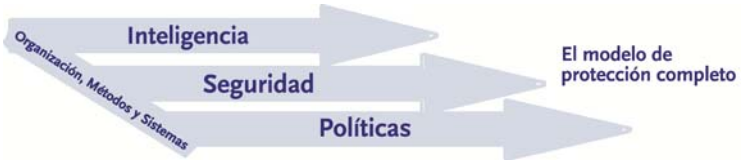
Organización

La estructura de una organización de gestión de riesgos de la información varía dependiendo del tipo de negocios que lleve a cabo, o del tipo de servicios que preste. Sin embargo, existen varios aspectos comunes a toda el área.

En términos generales, las funciones relacionadas con la prevención y reacción ante el delito electrónico deberían integrarse en la entidad responsable de la reacción, medición y mitigación de riesgos de la información. Esta entidad debería constituir una sola estructura, y debería trabajar de forma homogénea (ver la ilustración funcional, abajo).

El combate contra el delito electrónico como conjunto de amenazas requiere, naturalmente, una gran capacidad de inteligencia (en el sentido gubernamental/militar) y de investigación, así como de capacidad de reacción.

Tradicionalmente existen tres líneas de reacción utilizadas frente al crimen, y que deberían ser adoptadas para el combate del delito electrónico:



La **'Inteligencia'** es básicamente una herramienta estratégica.
La **'Seguridad'** se centra en la capa táctica (funcional) de la organización.
Las **'Políticas'** se utilizan fundamentalmente en el nivel operacional.

Estas afirmaciones son muy generales y, obviamente, los tres grupos de actividades han de desarrollarse en los tres niveles de la organización, en diferente grado.

Por ejemplo, en el caso de un sistema de **inteligencia** de amplio espectro, éste es concebido y desarrollado en los niveles táctico y operativo, con aportes de usuarios en el nivel estratégico. Sin embargo, una vez que entra en uso, los principales usuarios son la Junta Directiva (la 'primera línea de defensa'), sus analistas de planificación estratégica y asesores expertos, aunque también existirían beneficiarios indirectos a lo largo de toda la jerarquía de la empresa.

La **seguridad** de la información de la organización siempre se define en el nivel táctico (la 'segunda línea de defensa'), y también desde este nivel se mantiene, mejora, evalúa y mide el marco resultante. La supervisión, sin embargo, debería lograrse en el nivel superior, el estratégico. De ahí el nombre: 'primera línea de defensa'.

Las **políticas** se enmarcan en la 'tercera línea de defensa', por medio de equipos CIRT (Equipos de Respuesta para los Sistemas de Información Corporativos), que vigilan la aparición de software malicioso y las violaciones visibles de la seguridad, tanto interna como externa. Una unidad llamada DSA (Administración de la Seguridad de los Datos) también forma parte de este nivel. Esta unidad aporta varios servicios operativos, principalmente la provisión y cambio de permisos de acceso, la vigilancia de su buen uso, y lleva a cabo, junto con los equipos CIRT, las demás funciones relacionadas con la seguridad, la gestión de las claves criptográficas, etc. El rostro visible del DSA es a menudo parte del *HelpDesk*, lo cual otorga una apariencia más positiva y orientada al servicio a esas fuertes funciones de control. No obstante, tiene que haber 'vigilantes del cumplimiento' en los tres niveles de la organización.

Todo esto tiene que ser aplicado en los ámbitos de Prevención, Respuesta, Medición y Evaluación, no sólo como conceptos o buenas ideas a tener en cuenta en el trabajo. Para garantizar el éxito, este esquema tiene que formar parte de la estructura funcional (mi propio modelo funcional, ilustrado abajo, está basado en este enfoque).

Todo el marco organizacional, metodológico y sistémico/tecnológico ha de hacer énfasis en la **Prevención** como enfoque clave, al cual se debe dedicar aproximadamente el 75% del presupuesto y del esfuerzo. La **Respuesta** debe utilizar otro 15%, y la parte de **Medición/Evaluación** el 10% restante. La **Medición** solía ocupar el 5%, pero el desarrollo normativo que se ha dado en los últimos años ha incrementado el nivel de recursos que se requieren, y hoy en día incluso esta estimación probablemente se quede corta.

Estos porcentajes son generales, y varían entre distintas organizaciones. Esto se debe principalmente a limitaciones practicas de índole local o específicas a un tipo de negocio, que imposibilitan la prevención de problemas e incidentes, y que, por tanto, necesitan el apoyo de operativos de respuesta altamente cualificados (otra vez los equipos CIRT, integrados a las demás funciones orientadas a garantizar la continuidad del negocio).

Los anteriores párrafos han descrito en líneas generales el tipo de organización interna que se necesita para combatir y gestionar el delito electrónico y los riesgos de información generados de forma accidental.

Por desgracia, hay otra necesidad que no puede ser ignorada: la necesidad de que exista un alto nivel de comunicación, o incluso integración, con las funciones externas e internas que afectan al riesgo de delitos electrónicos. Esta es un área en la que los que trabajamos en la 'industria' de la protección de información a menudo fallamos, tendiendo a parcelar demasiado el trabajo, y a pasar la responsabilidad a otros, en lugar de compartir y abordar conjuntamente el trabajo.

Alianzas e integración

Internamente, es fundamental que los proveedores de Tecnologías de la Información y la Comunicación (TIC) sean parte de la gestión de riesgos electrónicos, en cada uno de los tres niveles arriba mencionados, para la planificacion de servicios, el desarrollo y la medición del nivel de servicio (*no* – como se vio antes – como un grupo de funciones culturalmente separadas a las cuales se les puede 'pasar la responsabilidad').

Lo mismo puede decirse de la relación entre un proveedor TIC con gestión de riesgos y el negocio al que provee. El gerente de un negocio es el dueño de sus riesgos (todos ellos), y no puede delegar esta responsabilidad o externalizarla. Sí puede, por supuesto, delegar la operación y el mantenimiento

de los mecanismos de control que ha encomendado a ciertos 'guardianes'; de hecho, en el caso de ICT, se dará cuenta de que es absolutamente necesario hacerlo. En este caso, el dueño del riesgo de negocio sigue siendo responsable y los 'guardianes' a su vez responden ante él (haría falta otro artículo para describir esta relación en la práctica). Además, debería buscar el aporte de especialistas que puedan ayudarle a tomar decisiones relacionadas con la gestión de riesgos, y si se ha tomado una decisión acerca del control, a clasificar los activos adecuadamente y establecer los mecanismos de control que han de ser utilizados. Esto, naturalmente, se debe llevar a cabo con la ayuda de especialistas y dentro de la estrategia de protección de la información definida por la Junta.

Gracias a la estructura 'de abajo a arriba', el negocio puede utilizar aportes de las diversas entidades externas y gestionar el riesgo que algunas de ellas presentan.

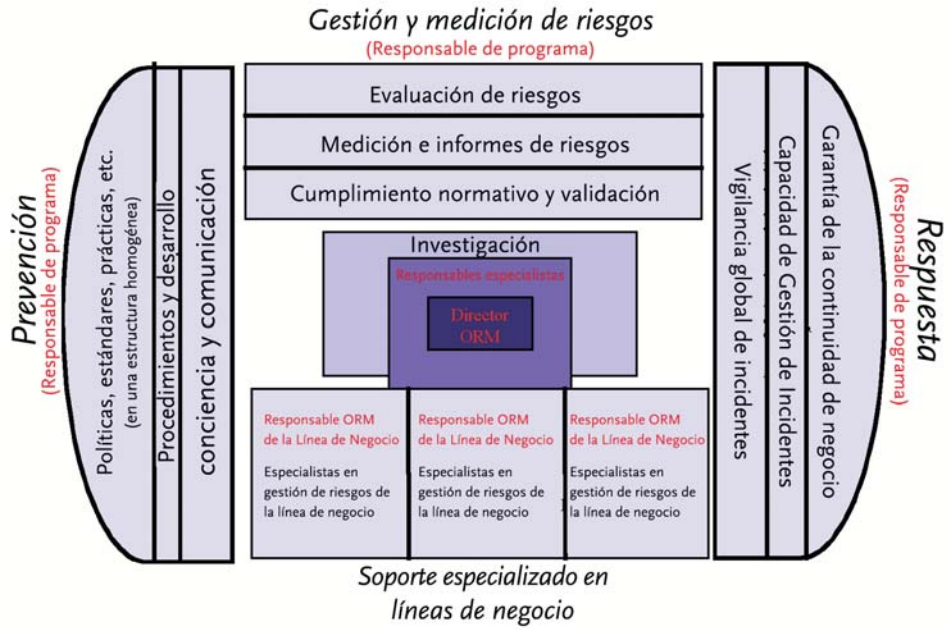
La convergencia de diversas actividades relacionadas con la gestión de riesgos con el fin de formar una 'división' de gestión de riesgos plenamente integrada en la empresa no es tarea fácil, y debería formar parte de un amplio programa de gestión de cambios que garantice que cada sección especializada esté funcionando correctamente, antes de llevar a cabo la integración. No obstante, es más fácil lograr la convergencia de las funciones no relacionadas con la gestión de riesgos financieros, siempre y cuando se haga frente a este nivel de convergencia de modo funcional, y no de 'silo' a 'silo' (es decir, intentado unir varios grupos cercanos organizacionalmente en lugar de funcionalmente).

En el enfoque de gestión de riesgos no financieros, el papel principal, nos guste o no, corresponde a la gestión de riesgos de la información, la cual incluye los esfuerzos contra el delito electrónico.

Los riesgos de proceso, los riesgos de control, los riesgos de recursos humanos, etc., todos ellos comparten, en el nivel más bajo y básico, **la necesidad de proteger información.**

En definitiva, no se resistan al hecho de que la información es el recurso predominante. Adóptenlo y desarrollen un modelo de convergencia basado en la funcionalidad de la gestión de riesgos de la información, expandan este modelo en el modo que resulte más practico para su organización, y después añadan el residuo de funcionalidad de gestión de riesgos no financieros – descubrirán que será mucho mas pequeño de lo que imaginaban. El siguiente diagrama es mi propio modelo funcional generalizado.

Modelo funcional de convergencia para la gestión de riesgos no financieros (incluye la gestión del delito electrónico)



No intenten forzar la convergencia vertical de la gestión de riesgos no financieros (seguridad física, gestión de riesgos informáticos, riesgos de proceso, riesgos de calidad, riesgos normativos, etc.) simplemente obligando a estas funciones a trabajar conjuntamente y a las personas a sentarse al lado las unas de las otras.

La convergencia se debe afrontar lateralmente, desde los elementos básicos de la gestión de riesgos **(Prevención, Respuesta y Medición/Evaluación),** y añadiendo posteriormente el siguiente nivel de detalle. A continuación se debe sumar la gestión tradicional y asegurarse de que se gestione y estandarice el conocimiento especializado, que es un requisito fundamental.

Los equipos de gestión se establecen de forma casi natural. En organizaciones de gran tamaño, será necesario dividir los equipos de gestión en "Estrategia y Administración", "Gestión de Programas" y "Operaciones". Sin embargo, el modelo se puede adaptar a cualquier tamaño y tipo de gran organización, y, simplemente como concepto, incluso puede ser aplicado a PYMEs.

Si el proceso de cambio hace frente de forma explicita y exhaustiva a las cuestiones vinculadas al 'factor-x' (personalidad/subjetivas) que surgen en cualquier proyecto de reconstrucción de un equipo, será posible lograr la estructura matricial de gestión perfecta.

MATÍAS BEVILACQUA
• Director Tecnológico · Cybex

¿QUÉ ES EL COMPUTER FORENSICS?

El Computer Forensics o Análisis Forense de Dispositivos Digitales es, como su propio nombre indica, una rama específica de la ciencia forense. Lo cual, nos lleva a la definición del concepto de ciencia forense que no es otra que la de la aplicación de una o múltiples disciplinas científicas – basadas en el método científico – dentro de un proceso jurídico. Esta definición básica nos permite vincular directamente el método científico con el mundo jurídico. Por ello, toda ciencia forense centra su campo de actividad en los principios que rigen la detección, aseguramiento y análisis de las pruebas con el fin de garantizar en última instancia la admisibilidad de las mismas. Habiendo contextualizado las ciencias forenses es simple ver el análisis forense de medios digitales como una extensión de la aplicación de las técnicas forenses al creciente entorno digital que nos rodea. Las técnicas más elementales empleadas en el análisis forense de medios digitales nacieron prácticamente con la propia tecnología. Este fenómeno – atípico entre las disciplinas forenses – se debe a un simple motivo; la que nos ocupa es una de las pocas ciencias forenses en las que el sustrato que sustenta la prueba ha sido creado por el hombre. Esto impone una paradoja interesante. El mismo progreso de toda ciencia forense persigue en última instancia un conocimiento en mayor profundidad del objeto de análisis de su disciplina y del entorno en el cual se encuentra el mismo. Dicho conocimiento repercute en un incremento en la capacidad de identificación, interpretación, correlación y en un sinfín de propiedades adicionales que en definitiva permiten que la disciplina forense obtenga cada vez más información o bien información de mayor valor añadido. En el caso que nos ocupa por el contrario (el computer forensics), podría argumentarse que el conjunto global de seres humanos necesariamente tiene en su poder el conocimiento exhaustivo del objeto de estudio y de su entorno. Es decir, dado que el análisis forense de medios digitales tiene por objeto de estudio la tecnología, y la misma ha sido creada por el hombre, puede concluirse que no debería haber evolución posible dado que partimos de un conocimiento absoluto (por definición) del objeto de estudio y de su entorno. Por fortuna o por desgracia esto no es así. Lógicamente, si bien puede que la suma del saber humano permita un conocimiento exhaustivo de la tecnología, lo cierto es que el conocimiento individual o empresarial dista mucho de aproximarse a esa hipotética suma del conocimiento humano. No obstante, esta aparente paradoja es una de las explicaciones del acelerado ritmo de evolución de nuestra disciplina forense en los últimos años.

Origen

Históricamente, la aparición de las primeras herramientas específicamente creadas como ayudas al análisis forense se sitúan en los años 80 como parte de una serie de iniciativas del CART (Computer Analysis and Response Team) del laboratorio de ciencias forenses del FBI. No obstante, el origen de las técnicas y procedimientos básicos que conforman hoy en día los pilares fundamentales del computer forensics fueron creados por programadores a medida que creaban y expandían los límites de la propia tecnología. Podemos realmente hablar de las primeras herramientas forenses refiriéndonos a las propias herramientas internas creadas por el equipo de desarrollo para evaluar, validar y probar su tecnología. Lógicamente, en ese momento no eran llamadas herramientas forenses pero la esencia es la misma, a pesar de que el uso fuese bien distinto. Sin ir más lejos, a día de hoy una parte considerable (aunque en constante declive) del "kit de herramientas" de un analista forense siguen siendo herramientas de apoyo (de administración, de recuperación ante errores, de monitorización avanzada...) creadas por los mismos desarrolladores de una u otra tecnología. En cierta medida se puede ir evaluando el grado de madurez de la capacidad forense disponible sobre una tecnología dada analizando el tipo de herramientas empleadas habitualmente por los analistas forenses. Por ejemplo, en el análisis forense de sistemas de ficheros muy extendidos como pueden ser FAT o NTFS se emplean, hace ya muchos años, herramientas forenses a medida. En un grado intermedio de madurez, tendríamos el terreno del análisis forense sobre teléfonos móviles. Hasta hace relativamente poco se empleaban herramientas destinadas a otros usos (generación de backups o liberación de terminales, por ejemplo) y sólo en los últimos años han comenzado a aparecer tímidamente herramientas específicas destinadas a este sector. Por último tenemos en el otro extremo tecnologías como SCADA o el emergente terreno del llamado HW forensics para las cuales únicamente se dispone de herramientas que son más propias de un desarrollador que de un analista forense.

Evolución

Podríamos hablar de la evolución del computer forensics desde múltiples ópticas interesantes.

Volumen de datos

No podemos obviar el que tal vez sea el aspecto evolutivo con mayor presencia en la mente de todo analista forense: el incremento del volumen de datos a procesar. La ley de Moore, por la cual cada dos años se duplica el número de transistores por circuito integrado, inspiró en su día la ley de Kryder por la cual se duplica anualmente la densidad de información en los dispositivos de almacenamiento electromagnéticos. A pesar de que recientemente se dudaba de la ley de Kryder, el anuncio de Hitachi de comercializar discos de 4TB en 2009 nos indica que efectivamente parece seguir en pié. Y más

recientemente, tenemos de la mano de Nanochip Inc. la aparición de nuevas tecnologías que amenazan con superar la ley de Kryder alcanzando el TB por chip. De este ritmo frenético de crecimiento en los volúmenes de almacenamiento disponibles lo único por lo cual realmente hemos de preocuparnos es por la disparidad entre la ley de Moore y la ley de Kryder, que nos indica que el ritmo de crecimiento del volumen de almacenamiento electromagnético duplica el de la capacidad computacional. De ser así, la distancia entre la potencia de cálculo disponible y el volumen de datos a procesar crecerá a corto o medio plazo a dimensiones infranqueables.

Coste computacional

Habiéndonos atrevido a vaticinar una importante carencia de recursos computacionales para el análisis forense de medios digitales, es de obligado cumplimiento una breve reflexión sobre su evolución.

Tradicionalmente los recursos computacionales aplicados al análisis forense de dispositivos digitales han crecido de forma proporcional al incremento en el volumen de datos a procesar. Recientemente, no obstante, vemos un cambio muy importante en esta relación que amenaza con derivar en una tendencia exponencial. El ritmo de crecimiento en el consumo de CPU observado en un laboratorio forense es, nuevamente, un muy buen indicador de su nivel de madurez. Inicialmente, todo laboratorio centra su progreso en la obtención de más información a partir de un conjunto de bits y bytes determinado. Llamémoslo I+D+i "hacia abajo", interpretando cada vez estructuras de datos de menor nivel, descendiendo a través de las capas de abstracción creado por aplicaciones y sistemas operativos. Estas líneas de investigación derivan, salvo contadas excepciones, en un crecimiento de la demanda de capacidad computacional que es linealmente proporcional al incremento en el volumen de datos a procesar. A media que el laboratorio forense madura y se profesionaliza, el desarrollo de tecnología y conocimientos en las líneas de investigación "hacia abajo" chocan con limitaciones infranqueables. No podemos ir más allá del último bit. Una vez se ha desarrollado la tecnología para la interpretación de la información aportada por todos y cada uno de los bits que conforman un objeto dado, la filosofía de investigación "hacia abajo" muere por definición. Si bien no podemos ir más allá del último bit, dado que hemos descendido por todas las capas de abstracción obteniendo toda la información disponible, sí que podemos reenfocar el proceso y comenzar a añadir capas de abstracción, es decir, investigar "hacia arriba". Estas líneas de investigación se nutren de la aplicación de técnicas más propias de la minería de datos y en particular de la matemática estadística sobre la agregación masiva de información

forense. Y es precisamente este cambio de paradigma el que tiende a generar procesos con costes exponenciales sobre el volumen de datos a procesar.

Futuro

El computer forensics como ciencia forense que es, ha evolucionado y continuará evolucionando en la misma línea que el resto de disciplinas forenses. Todas las ciencias forenses se encuentran en continua evolución, constantemente buscando obtener más información y de mayor peso jurídico a partir de un conjunto finito (y habitualmente escaso) de pruebas. La relación que aparentemente existe y se mantiene entre el incremento de la capacidad computacional y el incremento en la densidad de almacenamiento digital nos plantea un futuro complejo. Sin lugar a dudas, encontraremos una salida a esta aparente paradoja, pero con toda probabilidad se redefinirá por completo nuestra forma de trabajar a corto o medio plazo.

STEFANIA DUCCI

- Responsable de la Unidad de Cibercrimen · Unidad de Crímenes Emergentes y Tráfico de Seres Humanos · UNICRI

EL INSTITUTO INTERREGIONAL DE LAS NACIONES UNIDAS PARA INVESTIGACIONES SOBRE LA DELINCUENCIA Y LA JUSTICIA (UNICRI) Y SUS ACTIVIDADES CONTRA LOS DELITOS INFORMÁTICOS

El Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia - UNICRI - fue creado en 1968 para asistir a las organizaciones intergubernamentales, gubernamentales y no-gubernamentales en la formulación e implementación de políticas avanzadas en las áreas de prevención de la delincuencia y de justicia penal.
En un mundo cambiante, los principales objetivos de UNICRI son avanzar en la seguridad, servir a la justicia y construir la paz.

En particular, UNICRI esta comprometida con la lucha contra el cibercrimen, el crimen organizado (especialmente el tráfico de seres humanos, drogas y armas), la corrupción y el terrorismo. Otras de las áreas en las que interviene son: la violencia, tanto doméstica como laboral; el crimen medioambiental; y la protección de víctimas y del legado cultural. Asimismo, UNICRI también lleva a cabo programas sobre la reforma de la justicia penal, con especial énfasis en la justicia penal juvenil.

Las principales herramientas de trabajo de UNICRI son la gestión del conocimiento, la creatividad a la hora de encontrar soluciones y el poder de sus socios. UNICRI opera en nichos selectos como un laboratorio de ideas, y sus actividades ayudan a integrar esfuerzos, tanto nacionales como internacionales, para identificar buenas prácticas y adaptarlas a los diferentes contextos nacionales.

Los objetivos de UNICRI son:

- ✓ Avanzar en el entendimiento de problemas relacionados con la delincuencia
- ✓ Fomentar sistemas de justicia penal justos y eficientes
- ✓ Apoyar el respeto a los estándares e instrumentos internacionales
- ✓ Facilitar la cooperación en la asistencia judicial y aplicación de la legalidad internacional

UNICRI se ve a sí mismo como el primer intermediario de respuesta. Ha adquirido protagonismo por su enfoque dinámico, fresco e innovador en el área de análisis de acciones aplicadas.
El programa de Investigación Aplicada de UNICRI está organizado en cuatro áreas principales de trabajo: Crímenes Emergentes y Tráfico de Seres Humanos; Gobierno de la Seguridad y Prevención del Terrorismo; Reforma de la Justicia; y Formación de Postgrado.

Las actividades contra el cibercrimen se llevan acabo en el marco de la Unidad de Crímenes Emergentes y Tráfico de Seres Humanos, y consisten en 2 proyectos: el *Hackers Profiling Project* (HPP), y la iniciativa SCADA y de Seguridad de las Infraestructuras Críticas Nacionales.

El *Hackers Profiling Project* (HPP)

Este proyecto busca mejorar las respuestas al crimen informático y al crimen organizado transnacional que puede estar involucrado en este tipo de delitos, mediante la elaboración de perfiles de los diferentes tipos de hackers, con especial énfasis en su posible participación en el crimen organizado transnacional y el ciberterrorismo. Al ayudar a comprender mejor a los hackers, el proyecto HPP contribuirá a la prevención y lucha contra los delitos informáticos y a la mejora de los métodos de detección de intrusos.

El proyecto, que comenzó en 2006, y cuenta con el apoyo de la Asociación Italiana de Seguridad Informática (CLUSIT), se compone de 8 fases:

Fase 1 – Recolección de material teórico (finalizada/en curso): Elaboración y distribución de un cuestionario (http://hpp.recursiva.org/) compuesto de tres módulos: Módulo A, datos personales; Módulo B, datos relacionales; Módulo C, datos técnicos y criminológicos. El cuestionario está disponible en varios idiomas.

Fase 2 – Observación (en curso): Participación en eventos sobre seguridad informática alternativa en Europa, EEUU, Asia y Australia.

Fase 3 – Clasificación (en curso): Creación de una base de datos para la clasificación y elaboración de datos recogidos en la fase 1.

Fase 4 – Obtención de datos "en vivo" (por comenzar): Elaboración y construcción de Sistemas *Honey-Net* de última generación adaptados.

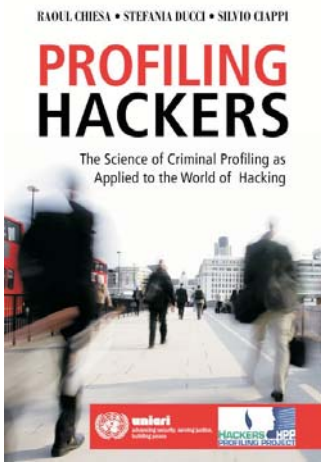
Fase 5 – Análisis y correlación (pendiente): análisis y correlación de datos obtenidos a través del cuestionario, Honey-Net y perfiles deducidos a partir de la literatura sobre el tema.

Fase 6 – Evaluación en vivo (pendiente): Evaluación continua de perfiles de hackers y correlación del *modus operandi* a través de datos recopilados en la fase 4.

Fase 7 – Finalización de los perfiles (pendiente): Redefinición y ajuste de los diversos perfiles de hackers previamente utilizados como "estándares de-facto".

Fase 8 – Difusión del modelo (pendiente): Elaboración de resultados finales, borrador y publicación de la metodología elaborada, campañas para generar conciencia.

El primer resultado del proyecto será la publicación del libro *Profiling Hackers. The Science of Criminal Profiling as Applied to the World of Hacking", R. Chiesa, S. Ducci, S. Ciappi, Taylor&Francis*, de próxima publicación (1ª edición italiana publicada por Apogeo en febrero de 2007).



SCADA y la Seguridad de las Infraestructuras Críticas Nacionales

El propósito del segundo proyecto, que comenzó en 2007, es crear herramientas informáticas para la evaluación de la seguridad y elaborar mejores prácticas y metodologías para incrementar la seguridad de sistemas informáticos con estructuras SCADA (Supervisory Control and Data Acquisition). Los entornos SCADA se aplican en sistemas que gestionan y controlan la producción de productos industriales, pero también son utilizados por plantas eléctricas y nucleares, instalaciones petrolíferas, proveedores de agua y gas, y los sectores de telecomunicaciones y transporte.

La gestión informatizada correcta y segura de estos sectores críticos es esencial para la estabilidad, seguridad y bienestar nacional, dado que este tipo de infraestructuras son probables blancos de ataques informáticos, tanto en el día a día como en situaciones de guerra informática.

Las fases del proyecto son: el análisis de las últimas tendencias en seguridad SCADA a través de entrevistas con empresas SCADA, el análisis de mejores prácticas a nivel internacional (ISO, NIST, etc.), el establecimiento de CriSTAL (*Critical Infrastructures Security Testing and Analysis Lab*), la implementación de la pagina web de Cristal (http://cristal.recursiva.org/), la elaboración de una metodología para poner a prueba la seguridad en entornos SCADA y, finalmente, el desarrollo de herramientas *ad-hoc* y metodología para evaluar la seguridad SCADA.

Para más información, por favor, contacten con la encargada de proyectos sobre cibercrimen, Sra. Stefania Ducci (ducci@unicri.it; Tel.: +39 011 6537157).

Para mas información sobre las actividades de UNICRI, por favor, visiten la página web: www.unicri.it

Sentencia nº 236/2008 de 9 de Mayo de 2008

- Sentencia sobre la validez de los rastreos informáticos realizados en la red por la policía y necesidad de autorización judicial para desvelar la identidad de las direcciones IP.

SUMARIO

En el marco de la celebración de un foro de Ciberpolicías, se realizaron - sin conocimiento judicial - rastreos de redes de intercambios de archivos que abocaron en un listado de IP desde las que se había tenido acceso a archivos con contenidos ilícitos. El listado se presentó ante un juzgado para solicitar el mandamiento destinado a los proveedores de servicios de Internet para la identificación de los titulares de las IP. La sentencia de instancia fue absolutoria para la acusada del delito de facilitación del material pornográfico infantil - titular de una de las líneas identificadas - tras declarar la nulidad de la prueba por estimar vulnerado el secreto de las comunicaciones en la obtención de las direcciones IP al no haber contado con autorización judicial.

Dicha sentencia fue recurrida por el Ministerio Fiscal quien, entre otros, señala las diferencias existentes entre el acceso a las comunicaciones telefónicas tradicionales y los métodos de acceso a Internet. El Tribunal Supremo en la resolución analizada dicta la nulidad de la sentencia combatida al determinar que el acceso a la información (direcciones IP) puede efectuarla cualquier usuario. Indicando también que no se precisa autorización judicial para conseguir lo que es público y cuando el propio usuario de la red es quien lo ha introducido en la misma. Continúa afirmando que las IP son datos públicos en Internet, que no se hallan protegidos por los artículos 18.1 y 18.3 CE.

Sentencia nº 1028/2007 de 11 de Diciembre de 2007

- Sentencia sobre falsedad en documento mercantil y apropiación indebida. Apertura de manera informática de una cuenta corriente y realización de operaciones.

SUMARIO

El acusado - director de una oficina bancaria - abrió una cuenta corriente informática a nombre y titularidad de una persona ya fallecida, desde la que realizó diversas operaciones financieras (venta de fondos, retirada de dinero y compra venta de acciones) sin conocimiento ni consentimiento de los herederos. La sentencia impugnada señalaba la atipicidad de las conductas, absolviéndolo de los delitos de apropiación indebida, estafa, falsedad y descubrimiento y revelación de secretos.

El Tribunal Supremo sin embargo retiene el recurso de casación en cuanto a la falsedad documental, al considerar que el acusado simuló la participación de personas en operaciones en las que no habían intervenido. Considera el Alto Tribunal que incurrió en responsabilidad penal por falsedad de documento mercantil en tanto fingió en dichos actos la intervención de personas que eran las únicas autorizadas para realizar o autorizar tales operaciones de disposición de bienes, condenándolo por un delito continuado de falsedad en documento mercantil en concurso con un delito continuado de apropiación indebida.

Del 11 al 12 de Septiembre de 2008
(ISOI) Internet Security Operations. *Tallinn, Estonia.*

- DA y MWP (comunidades de lucha contra los botnets) organizan la 5ª edición de estas jornadas anuales que versarán sobre temas como respuestas a incidentes en Internet, fraude cibernético e investigaciones, y casos prácticos del cibercrimen.

Del 23 al 25 de Septiembre de 2008
(IMF) 4th International Conference on IT Incident Management & IT Forensics 2008. *Manheim, Alemania.*

- "Security Intrusion Detection and Response" (SIDAR) organiza esta conferencia anual que pone al servicio de expertos de todo el mundo una plataforma para discutir acerca de áreas de manejo en seguridad de incidentes tecnológicos y análisis forenses. El IMF incentiva la colaboración e intercambio de conocimientos entre empresarios, académicos, servicios de seguridad del estado y otros cuerpos gubernamentales.

Del 30 de Septiembre al 1 de Octubre de 2008
BA- Con 2008. *Buenos Aires, Argentina.*

- Primera conferencia anual sobre seguridad tecnológica aplicada. Eminencias internacionales y de Suramérica en el ámbito de seguridad industrial compartirán sus conocimientos tecnológicos. Temas como los nuevos descubrimientos sobre redes informáticas de ataques y defensas de hacks, soluciones de seguridad comercial y experiencia en seguridad internacional, se pondrán a debate mediante sesiones tutoriales.

Del 6 al 8 de Octubre de 2008
VI Seminario de Pruebas Electrónicas. *Madrid, España.*

- Seminario anual organizado por Cybex y el Consejo General del Poder Judicial. Magistrados y fiscales del Tribunal Supremo, el jefe de la unidad de cibercrimen del Consejo de Europa e ingenieros informáticos expertos en la materia, entre otros, revelarán la importancia de la prueba electrónica desde su detección hasta su presentación en los tribunales. Abierta la inscripción.

CYBEX agradece las contribuciones realizadas por los colaboradores para la confección de este Newsletter mensual. Recordamos a los lectores que las opiniones y comentarios publicados en estas páginas reflejan la perspectiva del autor que firma el escrito.

• Para obtener más información sobre CYBEX, consulten la página: http://www.cybex.es