



Ahora leer te costará muy

Lunes, 11 de octubre de 2004

Webmail | Alertas | Envío de titulares | Pr

PORTADA | ACTUALIDAD | ECONOMÍA | DEPORTES | OCIO | CLASIFICADOS | SERVICIOS | CENTRO COMI

[SECCIONES]

■ SOCIEDAD

Local

Regional

Opinión

Nacional

Internacional

Dinero y Negocios

Deportes

Sociedad

Cultura

Gente

Televisión

Titulares

Tecnología

Femérides

Viñetas

Especiales

[PARTICIPA]

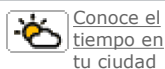
Foros

Chat

[CANALES]

Seleccione...

EL TIEMPO



SOCIEDAD

## Arbitraje «on line» de litigios entre empresas

**Aumenta la pena a dos años de prisión por el intercambio de ficheros con derechos de autor a través de redes P2P**

MARTA VILLALBA/MADRID

La Asociación Comunitaria de Arbitraje y Mediación (ACAM) tiene previsto inaugurar para junio de 2005 un servicio de arbitraje de litigios entre empresas a través de internet. Desde la web [www.arbitraje-acam.org](http://www.arbitraje-acam.org), tanto personas asociadas como no van a poder solicitar el arbitraje, enviándose toda la documentación por correo electrónico. Se va a poder realizar mediante internet todo el proceso, desde la solicitud hasta el laudo final.

Para asegurar la identidad de los implicados en el litigio, y que el sistema sea inviolable, la ACAM expedirá su propio certificado electrónico para cada uno de los intervinientes, y que sólo servirá para ese procedimiento en concreto.

Con esta forma de arbitraje, además eliminar la dependencia física de los implicados en el litigio y de acelerarse todo el proceso, ya que las comunicaciones son en tiempo real (las tres partes pueden acceder a todos los documentos), las tarifas por el servicio son un 50 por ciento más baratas (en algunos casos más) que de la forma tradicional. No existe en el mundo ninguna iniciativa de arbitraje como la que la ACAM va a poner en marcha. Con la reforma del Código Penal, que entró en vigor el pasado viernes 1 de octubre, al que pillen descargándose en el ordenador archivos con derechos de autor de las redes de intercambio «peer to peer» o P2P, le pueden caer entre seis meses y dos años de prisión (antes la máxima pena era de un año). Este delito es el más frecuentemente cometido por los empleados desde el PC del trabajo (el 31 por ciento de los casos), según un estudio de PricewaterhouseCoopers, que ha analizado 393 casos de infracciones llevadas a cabo en empresas españolas, utilizando los recursos informáticos de la compañía.

Sin embargo, esta práctica ilegal suele ser perdonada por las empresas, que responden extremando las medidas de seguridad: bloquean los puertos del servidor «firewall» para impedir que se utilicen estas redes de intercambio.

Averiguar que un trabajador o cualquier persona está descargándose archivos (copias) ilegales es muy fácil. Basta con intervenir la

Imprimir | Enviar

CASOS REALES

AHORA ES DELITO...

Una telefonista-recepcionista, adicta al Messenger, se pasaba el 40 por ciento de su jornada laboral usando esta aplicación. Fueron los propios clientes los que denunciaron que no atendía su trabajo. La empresa abrió una investigación interna. La empleada reconoció su adicción y aceptó una baja voluntaria.

La secretaria de un departamento comercial enviaba por correo electrónico a su novio información sobre los pedidos y las solicitudes de presupuesto de los clientes de la empresa. El novio, por sistema, mejoraba la oferta al cliente. Lo denunciaron los propios clientes. La trabajadora aceptó el despido procedente, al comprobarse la veracidad de los hechos examinando el correo electrónico. A través del «e-mail» corporativo estaba cometiendo un delito de revelación de secretos.

Un empleado de una agencia de publicidad, aprovechaba las campañas que hacía en la empresa para hacer otras para sus propios clientes, que él mismo facturaba. Una intervención en su PC desveló que había creado un directorio para cada cliente. Una simple comprobación de los gráficos que hacía para las campañas, en el formato de imagen JPG, se vio que llevaban el mismo número de serie («Unic user identification» o Número único de usuario) que los trabajos de la empresa. Un directivo de la empresa se percató de las similitudes gráficas de una de las campañas al verla en la prensa. Aceptó la baja voluntaria.

Un programador de una prisión, que gestionaba el saldo de los monederos electrónicos de los reclusos, programó una bomba lógica para que las tarjetas dejaran de funcionar después de ser baja en el empleo. Hubo una denuncia y se le intervino el código fuente en el

BUS

HOY

Hoy

Her

INT

kaz

Cate

dirección IP y ver el tráfico que tiene. Todo queda en el disco duro. Además, la policía puede investigar de oficio (sin denuncia previa del perjudicado).

#### Respuestas

Las Asociación de Usuarios de Internet (AUI), la Asociación de Internautas (AI) y la Federación de Consumidores en Acción (Facua) han puesto el grito en el cielo porque consideran que el intercambio de archivos no es delito si no existe ánimo de lucro. Pero Javier Ribas, responsable del grupo de Derecho de Tecnologías de la Información de Landwell-PwC, es contundente: «El intercambio de ficheros a través de P2P no es un delito, pero sí lo es si los archivos intercambiados contienen obras sujetas a derechos de autor como películas, canciones o trabajos de la empresa, independientemente de si se descargan o no con ánimo de lucro. Numerosas sentencias del Tribunal Supremo así lo avalan».

La segunda infracción más cometida en el puesto trabajo (22 por ciento), es la creación de empresas paralelas utilizando los recursos informáticos (correo electrónico, cuentas ftp...) para el trasvase de activos inmateriales e información, indica el informe. «Esto es muy común en programadores y analistas de sistemas de empresas desarrolladoras de software», apunta Javier Ribas. «Sucede cuando hay cierto desequilibrio entre los socios inversores capitalistas y los creativos. Al cabo de unos años, si la gestión no es correcta, los desarrolladores de software se dan cuenta de que ese trabajo lo pueden hacer por su cuenta. Se dejan llevar por la tentación, y van pasando activos inmateriales (el código fuente de los programas que comercializa la empresa), y es cuando cometen una infracción de los derechos de propiedad intelectual», señala Ribas.

Las amenazas, calumnias e injurias están tipificadas como delito, independientemente del soporte utilizado. El uso del correo electrónico corporativo para enviar estas afirmaciones es la tercera infracción más detectada entre las empresas españolas estudiadas por PwC (21 por ciento).

Normalmente, se envían a personas ajenas a la empresa y para difundir rumores negativos sobre la compañía con el fin de conseguir un traspaso de clientes. Los trabajadores deben saber que estos mensajes de correo electrónico con fines particulares pueden comprometer a la empresa, ya que la que figura es la dirección de «e-mail» corporativa. Sin embargo, es a través de chat y foros de internet donde este delito es más profusamente ejecutado. Pero bajo el anonimato que el empleado cree tener, subyace la dirección IP de la empresa, por lo que ésta queda vinculada a las afirmaciones.

El 11 por ciento de los casos analizados está relacionado con daños informáticos, habitualmente producidos como venganza a un conflicto laboral o un despido considerado injusto por el trabajador. Este delito consiste en destruir, alterar o inutilizar datos, programas o cualquier otro activo inmaterial albergado en redes, soportes o sistemas informáticos de la empresa. Suelen venir en forma de virus, sabotajes electrónicos y bombas lógicas (cuando el trabajador programa el sistema para que el daño se ejecute posteriormente a su baja).

El uso abusivo de los recursos informáticos, por ejemplo, navegar en exceso por internet, también es una infracción muy habitual. Y peligrosa, si se tiene en cuenta que al entrar en determinadas web, es posible que se acomode en las entrañas del ordenador un programa espía («spyware»), sin que el internauta se percate. Estos programas, también vienen camuflados en tarjetas postales electrónicas, o cuando se instala un programa P2P, y recopilan información del sistema en el que se descargan, que luego es enviada a través de la Red. De esta manera, y sin que el usuario sea consciente, se desvelan datos confidenciales del usuario. El estudio, elaborado de 2001 a 2003, destaca que este fenómeno ha aumentado considerablemente. La dirección del correo electrónico corporativo es personal y no se puede facilitar a otras personas sin el consentimiento del propietario.

Datos confidenciales

ordenador de su casa. Todavía está pendiente de sentencia. Sería un delito de daños informáticos.

Un administrador de sistemas fue despedido y dejó instalado un virus del tipo troyano. Al cabo de unos meses, desde su casa, entró en el correo electrónico del presidente de la compañía y reenvió todos los mensajes confidenciales al principal competidor. Se comprobó mediante una investigación su relación con los hechos por la dirección IP. Aún está pendiente de sentencia. Eliminar la protección anticopia de cualquier tipo de obra en soporte digital (antes de la reforma del Código Penal sólo estaba penado este delito cuando se rompía esta protección en un programa de ordenador). Compartir un acceso a internet. Esto es cuando dos o varios vecinos instalan un 'router' Wi-Fi para navegar pagando sólo una conexión. Compartir o descodificar de forma no autorizada la señal de un servicio protegido. Por ejemplo, la señal de una televisión digital como Digital +.

El siguiente delito más perpetrado (10 por ciento) es el de la revelación de información confidencial de la empresa o de datos personales de trabajadores y clientes. En este caso, se trata de acceder sin autorización a la información para manifestarla a terceros, generalmente competidores o clientes. Algunas veces, quien lo comete es un empleado con acceso a los datos, pero con obligación de reserva.

Las infracciones a la propiedad industrial (3 por ciento) se producen generalmente mediante el registro de un nombre de dominio de la empresa. En ocasiones los trabajadores van más allá: crean la web con contenido ofensivo para desprestigiar a la empresa o con el fin de obtener dinero por la transferencia del dominio.

En última posición, se sitúa la copia de activos inmateriales de la empresa, especialmente obras protegidas por la propiedad intelectual, para cederlas a terceros. En algunos casos se ha llegado a introducir la información en las redes P2P (2 por ciento).

Una vez descubierta la infracción, la estrategia seguida por el 78 por ciento de las empresas analizadas fue abrir una investigación interna, el resto se decantó por una investigación externa. Si una empresa detecta alguno de los delitos comentados, es conveniente que proceda según el artículo 18 del Estatuto de los Trabajadores: la intervención de los elementos personales del trabajador debe hacerse en horario laboral y estando presente el trabajador o algún representante sindical o del comité de empresa. Al trabajador no se le puede humillar ante sus compañeros en el transcurso de la intervención. Sólo el 26 por ciento de las infracciones detectadas acabaron en los tribunales. La mayoría (74 por ciento) de las empresas optaron por un acuerdo transaccional. Y únicamente el 13 por ciento de las compañías divulgó el delito. P2P

Subir



© Copyright HOY DIGITAL  
EDICIONES DIGITALES HOY, Sociedad Limitada Unipersonal. CIF: B06335467  
Carretera de Madrid-Lisboa, número 22 06008 BADAJOZ  
Registro Mercantil de Badajoz, Tomo 220, Folio 66, Hoja BA 11365  
Contactar / Mapa web / Aviso Legal / Política de privacidad / Publicidad / Master El Correo /  
Club Lector 10

Power