

Reunión del Comité de Ética de eMadrid (S2009/TIC-1650)

Facultad de Psicología, UNED (Madrid), 12 de abril de 2011

Acta de la reunión

Asistentes

- Manuel Castro, UNED
- Francisco Saiz, UAM
- Pilar Sancho, UCM
- Gabriel Díaz, UNED
- Jesús González Barahona, URJC
- Oscar Martínez Bonastre, UPM
- Carlos Delgado Kloos, UC3M

Desarrollo de la reunión

Informe del coordinador Gabriel Díaz

A las 10.30 comienza la reunión del Comité ético, coordinado por Gabriel Díaz, para velar por el cumplimiento de los derechos de todos los participantes en cualquiera de las plataformas de e-learning que se usen en el contexto de este proyecto, en lo que tiene que ver con cualquier aspecto relacionado con la seguridad informática.

En primer lugar el coordinador presentó el blog del comité y se comprobó que todos los presentes lo conocían y habían accedido a él. Con el fin de darle la visibilidad requerida, se decidió pedir al técnico de comunicación que colocara en la página de entrada a la web de eMadrid un enlace directo al blog del comité, y que en el apartado “Acerca de” coloque también la composición del comité y otro enlace al mismo blog. Con esto se busca una mayor participación de los miembros de eMadrid. De esta labor quedó encargado Gabriel Díaz.

Seguidamente se comentaron varios aspectos interesantes, y para algunos novedosos, sobre la información contenida en el documento sobre mínimos de cumplimiento de la LOPD en universidades. Se acordó que cada miembro informaría de cuál es la unidad administrativa que es responsable del cumplimiento de la LOPD en cada universidad. Jesús G. Barahona se compromete a tener listo su informe cuanto antes.

Se contó con la presencia de D. Enrique Rodríguez Martín, inspector jefe de la sección operativa 1ª de la Brigada de Investigación Tecnológica, que amablemente respondió a las preguntas de los presentes.

Manuel Castro comenzó preguntándole qué temas podrían ser de nuestro interés.

D. Enrique Rodríguez Martín contestó que en la Brigada tienen un grupo de seguridad que investiga los ataques que se producen, pero desde un punto de vista policial, no preventivo. Cuando se produce un ataque tratan de identificar a la persona, es entonces una investigación a posteriori más que preventiva.

Manuel Castro comenta que así se permite cerrar el ciclo, ya que tenemos una legislación que dice como se deben proteger los sistemas.

D. Enrique Rodríguez Martín añade que la seguridad es arbitraria, hay empresas que tienen una seguridad mínima, y hay otras que se lo toman más en serio porque saben que es el mayor problema que pueden tener. Así, por una parte está la legalidad, y por otra, lo que permite garantizar los sistemas.

Manuel Castro le pregunta que si, aunque actúen ante un ataque, la agencia de protección de datos cuenta con ellos para garantizar la seguridad, ya que él sabe que tienen sus propios inspectores. D. Enrique Rodríguez Martín responde que puede darse la situación de que por culpa de un ataque la agencia detecte que se ha incumplido la ley de protección de datos. Si el sistema de protección es bueno, siempre se detecta esa intrusión. Ahora, si esa vulnerabilidad es consecuencia de no cumplir la ley, la agencia va a decir algo, y ahí sí que ellos tienen que ver, son distintas actuaciones que están unidas por el mismo fin. Hay que señalar que hay empresas que no denuncian, tienen miedo a que ellos detecten algo y les multen, o que se descubra que es una empresa vulnerable y eso afecte a sus clientes. Por esta razón sólo tienen unas 18 o 20 denuncias al año.

Francisco Saiz le pregunta que si se ponen muchas sanciones y si alguna de ellas ha sido a alguna empresa educativa. D. Enrique Rodríguez Martín contesta que sí han puesto sanciones, y que por lo general son fuertes. Y además no se distingue, da igual el tipo de empresa. Añade que tenemos una ley de protección de datos de las más completas del mundo, tanto, que ellos mismos tienen problemas, por ejemplo cuando piden una dirección IP, ya que estos datos están protegidos. La ley lo tiene todo muy medido, y una facilidad, que es la consulta. Y hasta ahora no buscan responsabilidad civil subsidiaria, pero calcula que en un periodo de tiempo no demasiado largo sí lo harán.

D. Enrique Rodríguez Martín sigue diciendo que también hay que evaluar daños, para poder denunciar un hecho, tiene que haber un perjuicio, aunque esto no siempre es fácil, ya que hay que recuperar backups, etc. A veces el sistema sabe que alguien ha entrado, pero no sabe lo que ha hecho, si ha copiado, etc., hay que ver el tipo de hacker. Hay algunos que se saben mover y van a sitios y luego cuando salen eliminan todo rastro, luego hay otros menos detallistas. Cuanto menor es el rastro dejado, más sospechan que el hacker ha hecho algo importante. En la evaluación de daños se tiene todo esto en cuenta, cuánto tiempo ha estado el sistema parado, etc.

Añade también que por lo general el hacker no es una persona individual, normalmente hay alguien detrás que le dice lo que tiene que hacer, lo que le interesa de esa empresa.

Oscar Bonastre le pregunta si ha habido ataques desde fuera de España, a lo que D. Enrique Rodríguez Martín responde que esto es más difícil de investigar, ya que los servidores están en el extranjero, el que ataca utiliza ordenadores zombi, proxy, y es todo mucho más complicado. En este caso lo importante es parar el ataque, ya que cuanto más tiempo esté el sistema atacado, más riesgo corre. Esto lo hacen por comisión rogatoria, pero es un procedimiento muy lento, necesitan un requerimiento judicial, a través de exteriores, que se tiene que traducir, se manda a Justicia, en fin, que para cuando tienen todos los papeles el hacker ya se ha llevado todo lo que ha querido. Sin embargo, con Interpol tienen una relación más fluida y con decirles que hay una denuncia en trámite en un juzgado, deciden adelantar la investigación todo lo posible. Cuando la Brigada aquí tiene todos los datos de la investigación y necesitan actuar, piden permiso a los juzgados y normalmente lo obtienen.

D. Enrique Rodríguez Martín comenta además que si hay un proyecto a realizar no se debe sembrar el pánico, ya que realmente la seguridad no existe, cualquier antivirus detecta lo conocido hasta hoy, lo de mañana no se sabe. Hay muchas empresas que para protegerse sólo han aumentado el ancho de banda, pero por supuesto, no hay nadie a salvo.

Se le pregunta si también actúan en caso de que una empresa ponga información falsa a otra. D. Enrique Rodríguez Martín responde que sí, aunque previamente tiene que haber una denuncia, entonces analizan la información y con la Interpol buscan de donde ha podido entrar el ataque, aunque no siempre es fácil porque hay mucha información. También puede ser que las empresas no se den cuenta hasta dos meses después de que se haya producido el ataque. Normalmente hay un índice muy elevado de sospecha en una empresa de que el ataque viene del interior, de alguien que está o ha estado trabajando en ella. Por eso es importante actualizar claves, resetear, aunque sea un incordio, hay que cambiar claves, y que estas sean de garantía, alfanuméricas y sobre todo de números primos, esto es un gran sistema para reforzar la seguridad.

Oscar Bonastre le pregunta si se les dan ataques de ingeniería social.

D. Enrique Rodríguez Martín responde que sí, y que en la Brigada hay dos secciones, una de delitos contra las personas y otra de fraude en internet. Ahora han creado un grupo para el control de contenidos en internet, pero su funcionamiento es difícil. Son 45 personas y se apoyan en las jefaturas superiores, que manejan delitos informáticos, pero su mayor problema es la descentralización, y que el material que necesitan es muy caro y tienen que dotar de él a todos los equipos.

Se le pregunta también por temas de usurpación de personalidad, ya sea en la evaluación o que alguien haga un examen por otro. D. Enrique Rodríguez Martín recuerda que en la Universidad Carlos III hubo un ataque a actas hace 8 ó 9 años, y en la UNED también, por parte de un alumno que se cambiaba las notas. Recuerda que se detectó el ataque porque el profesor quiso hacer estadística de notas, y vio que habían cambiado resultados. El ataque interno es el más común, hay que reconocer que la protección exterior es fuerte, y es más fácil atacar un sistema desde dentro. También se cometen imprudencias cuando se dejan los ordenadores abiertos, mientras se va a tomar un café, por ejemplo, y en ese momento aprovechan para atacar el sistema. En este caso es entonces imposible localizar al autor de lo que se ha hecho. Añade que el delito es el mismo en la vida real que en internet, se puede delinquir una vez y escaparse, pero si repites, te pueden coger.

Oscar Bonastre comenta que en nuestro ámbito de trabajo puede ocurrir que si se examina online y hay suplantación de identidad, esto es una cuestión importante. D. Enrique Rodríguez Martín dice que el DNI electrónico ha solucionado mucho, pero Manuel Castro opina que no ha resuelto todos los inconvenientes, para ello habría que incluir temas de biometría, etc., que se van complicando, y al final resulta prácticamente imposible cubrir todas las variables. D. Enrique Rodríguez Martín comenta que, además, el coste económico es enorme, y al final resulta más barato llevar a la persona personalmente al lugar y examinarle, añade además que una posibilidad sería utilizar ordenadores “tontos”, que no hacen otras cosas, pero Manuel Castro dice que el nivel de complejidad necesario es enorme, y además carísimo.

D. Enrique Rodríguez Martín continúa diciendo que reciben muchas llamadas pidiendo asesoramiento, pero que esa no es su función, ya que si luego ocurre algo las empresas les responsabilizan. Ellos pueden dar recomendaciones generales, pero no asesoramiento legal ni personalizado, sólo sugerencias sobre buenas prácticas. En este sentido, siempre recomiendan que se ponga una denuncia, aunque normalmente la gente es reticente, ya que tienen miedo a las multas. Además añade que responden inmediatamente a los requerimientos de la agencia de protección de datos. A veces les preguntan a ellos, y otras veces se ven obligados a utilizar programas piratas, porque si no esa persona localiza tu procedencia, por eso tienen que entrar como ellos. Ahora dice que tienen muchas denuncias sobre problemas de telefonía con voz sobre IP, ya que es fácil de hacer y sólo detectan el ataque cuando ya se ha producido.

Y sin más asuntos que comentar, termina la reunión a las 13:00.

Firmas

- Manuel Castro, UNED
- Francisco Saiz, UAM
- Pilar Sancho, UCM
- Gabriel Díaz, UNED
- Jesús González Barahona, URJC
- Oscar Martínez Bonastre, UPM
- Carlos Delgado Kloos, UC3M