La Guardia Civil y el Mundo Digital

RAMON CORTÉS MARQUEZ

Comandante de la Guardia Civil

En esta intervención me centraré en algunos de los proyectos que lleva a cabo la Guardia Civil. Serán aquellos que más están relacionados con el mundo de la INTERNET, dejando de lado otros, relativos al mundo de las comunicaciones, que por su complejidad necesitarían ponencias específicas a cargo de especialistas.

A finales del pasado año, Guardia Civil organizó las I Jornadas sobre el delito cibernético en Barcelona. La buena acogida de las mismas, y las expectativas generadas en la sociedad nos animaron a trabajar a marchas forzadas en dos sentidos: la puesta en marcha de un Web propio en la INTERNET y la potenciación de la unidad de delitos informáticos. Una vez conseguidas estas metas, nos encontramos actualmente inmersos en otros dos proyectos, implantación de un WEB corporativo (intranet) y de un sistema de correo electrónico.

Pasemos a ver cada uno de estos proyectos, aún cuando sólo sea esquemáticamente, por necesidades del tiempo disponible.

Oficina INTERNET (ORIS)

El pasado 12 de marzo se presentó nuestro Web, con unas 400 páginas, quedando a cargo de la Oficina INTERNET, situada en la Oficina de Relaciones Informativas y Sociales (ORIS). En los ocho meses transcurridos ha recibido cerca de 33.000 visitas, que para un web de una fuerza policial es todo un récord. Las ventajas de nuestra incorporación a este mundo pueden verse desde dos puntos de vista: como parte de la administración pública y como parte de las Fuerzas y Cuerpos de Seguridad del Estado.

*Como parte de la Administración Pública.

La Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, ya apostaba por la abierta incorporación de las técnicas electrónicas, informáticas y telemáticas a la actividad administrativa y, en especial, a las relaciones entre los ciudadanos y la administración.

En concreto el artículo 45, especifica:

"1. - Las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de estos medios establecen la Constitución y las Leyes.

2. - Cuando sea compatible con los medios técnicos de que dispongan las Administraciones Públicas, los ciudadanos podrán relacionarse con ellas para ejercer sus derechos a través de técnicas y medios electrónicos, informáticos o telemáticos con respecto de las garantías y requisitos previstos en cada procedimiento".

La Guardia Civil, por tanto, se limita a aplicar dentro de su ámbito, la legislación vigente. En este aspecto, el servidor de la Guardia Civil, contiene páginas informativas, no sólo de carácter general sobre la Institución (estatuto, misiones, organización, servicios, historia, museo, etc.), sino que incluye información sobre cómo efectuar los trámites de armas, documentación que se necesita y donde dirigirse para realizarlos, lo que indudablemente evitará desplazamientos innecesarios al ciudadano y por lo tanto redundará en la calidad del servicio que se le presta.

No debe olvidarse que la Intervención Central de Armas de la Guardia Civil gestiona más de 3.500.000 de armas, que suponen un gran número de gestiones administrativas relativas a adquisiciones, licencias, renovaciones, etc. Todo lo que ayude a agilizar estos trámites será bien acogido por los ciudadanos.

Para profundizar en este último aspecto, la Guardia Civil se ha incorporado al proyecto Infoville, citado por anteriores ponentes. Se iniciará en Villena y aquellos otros pueblos que se unan al proyecto, un modelo de Puesto de la Guardia Civil acorde con el mundo de las comunicaciones digitales del futuro. Se pretende ofrecer al ciudadano todo un abanico de posibilidades que agilicen sus gestiones relativas a las armas. Se les notificará a sus buzones electrónicos la próxima caducidad de sus documentos, dándoles cita previa para su renovación, al tiempo que se les informa de los documentos necesarios; podrán efectuar consultas de cualquier tipo, referidas a cualquiera de los servicios que ofrece la Guardia Civil.

*Como parte de las Fuerzas y Cuerpos de Seguridad del Estado.

Ha pasado la hora de anunciar la llegada del mundo digital, de sus posibilidades y de sus peligros. Ya lo tenemos aquí y debemos prepararnos, o mejor dicho, ya debíamos estar preparados para hacerle frente. Por lo tanto, la Guardia Civil ha querido dar un paso adelante, ha apostado decididamente por incorporarse a ese mundo, ofreciendo información sobre delincuentes más buscados, obras de arte robadas, consejos útiles sobre cómo actuar en caso de robo, accidente o catástrofe, etc. Sin olvidarse de la posibilidad que tiene el ciudadano de ofrecer información a través del buzón electrónico.

Esta incorporación ofrece, además, la oportunidad, nada desdeñable, de introducir la "cultura digital" en la Institución. Su personal se verá motivado para abordar un perfeccionamiento en esta área, lo que facilitará su posterior incorporación a los grupos de investigación sobre delitos informáticos, superando el problema actual de falta de personal cualificado que padecen todas las fuerzas de seguridad.

Las principales policías del mundo disponen de personal especializado en Internet y delitos informáticos. La Guardia Civil está integrada en los principales grupos de trabajo que actualmente se llevan a cabo en Europa sobre el tema, como el de INTERPOL, algunos de cuyos integrantes tendrán ustedes oportunidad de escuchar en el panel de mañana. Esta integración potencia nuestras relaciones con

otros cuerpos policiales, que tan necesarias son para la persecución de las tramas delictivas en un mundo tan interdependiente como el actual.

La unidad de delitos informáticos

La otra faceta que ya se encuentra a pleno rendimiento es la unidad de delitos informáticos. Mañana tendrán oportunidad de conocer algunos de los numerosos servicios que ha prestado esta unidad en su corta existencia. Por mi parte, y sólo como mera introducción al panel de mañana, no hablaré de la unidad en sí misma, sino que les indicaré algunos de los fenómenos delictivos contra los que luchan, y de los cuales podemos ser víctimas cualquiera de nosotros al conectarnos a INTERNET.

HACKER: Persona que disfruta del reto intelectual de superar o rodear las limitaciones de una forma creativa. Su hobby consiste en entrar de forma ilegal en un sistema, para obtener información y presumir de ello. No conlleva la destrucción de datos ni la instalación de virus, pero pueden instalar "troyanos" que proporcionen passwords nuevos.

CRACKER: Es el hacker que utiliza sus conocimientos para obtener beneficios, o simplemente por causar daños. En realidad se trata de una división artificial, puesto que la línea que los separa es muy débil.

INSIDER: Es el empleado de una empresa, que generalmente actúa por venganza. Es el más peligroso y difícil de detectar.

Cualquiera de los anteriores puede ser utilizado por terceras personas para obtener información por motivos de espionaje industrial, o para hacer daño a la empresa rival.

Algunas de las herramientas software utilizadas son:

SNIFFERS: Programas encargados de interceptar la información que circula por la red. Por ejemplo: Cuando un usuario entra en un sistema, tiene que dar login y password. Estos datos viajan para ser comprobados con el fichero password y ahí es donde el sniffer actúa: intercepta estos datos y los guarda en un fichero para su utilización posterior de forma fraudulenta.

ROOTKITS: Es un programa que se encarga de borrar (zap) o enmascarar las huellas dejadas después de introducirse en un sistema. Estas huellas

se encuentran en los ficheros que guardan logs de lo que ha hecho un usuario (entrar, salir, ejecutar un programa, etc.).

TROYAN HORSE: Programa que se queda residente en el sistema que se pretende sabotear y que, o bien facilita información sobre lo que pasa en él, o ejecuta cambios sin que el usuario lo detecte. El "caballo de Troya" se utiliza para introducir otras formas de ataques, como los virus y las bombas lógicas. Es casi imposible asegurarse contra estos programas.

WORMS and VIRUSES: La diferencia entre el virus, conocido por todos, y los gusanos, es que éstos últimos son programas que se duplican ellos solos en un ordenador o en toda una red.

WAR DIALERS: Programas (demon) que escanean la línea telefónica en busca de módem para, a continuación, averiguar las palabras de paso.

LOGIC BOMB: Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá o modificara la información, o provocara la caída total del sistema.

SATAN (Security Administrator Tool for Analysing Networks): Programa que analiza una red determinada y detecta sus debilidades en seguridad. Está disponible en la red, como la mayoría de los citados anteriormente.

CRIPTER: No son delictivos en sí, pero se citan aquí por que son ampliamente utilizados por redes de delincuencia organizada para comunicarse entre ellos.

Web corporativo (intranet)

En estos días se está poniendo en marcha un web corporativo, que servirá de "tablón de anuncios" a nivel nacional. Será de uso interno y se podrá acceder a él desde cualquier terminal conectado a la red de Guardia Civil.

Sus posibilidades son idénticas a cualquier otro web de INTERNET. Cada Subdirección introducirá en él todas las disposiciones de interés que necesiten una distribución general. Así mismo podrá publicarse el Boletín Oficial de la Guardia Civil, que incluye destinos, cursos, etc.

Sistema de correo electrónico

Paralelamente a lo anterior, se trabaja en la puesta en marcha de un sistema de correo electrónico que sustituya las comunicaciones en papel. Este sistema se pondrá en marcha experimentalmente entre una Comandancia y la Dirección General, para ir extendiéndolo al resto del territorio nacional.

No puedo ocultar que la implantación de este sistema no será fácil. No se trata tan sólo de sustituir un sistema en papel por otro electrónico. Requerirá, por una parte un cambio de mentalidad de las personas dedicadas a trabajos burocráticos, y por otra un rediseño de los actuales canales de comunicación. Ambas cosas son importantes. La experiencia demuestra que la mayoría de los proyectos fracasan por la disposición contraria de los empleados hacia ellos.

En nuestro caso, debo reconocer que estamos llenos de vicios burocráticos. La información fluye, más lentamente de lo que desearíamos, debido a que pasa por escalones burocráticos que no aportan valor añadido al documento. Este trasiego sólo se justifica por el simple hecho de querer conocer todo lo que pasa en los escalones inferiores.

Pero debido a la acumulación de trabajo, se producen dos efectos no deseados: aumento del número de personas dedicadas a trabajos burocráticos y lentitud de los procesos. No voy a insistir más en este hecho, ya que estoy seguro que casi todos los funcionarios aquí presentes tienen ejemplos en sus propios departamentos.

Lo anterior, sin embargo, no debe dar una impresión falsa. De hecho su mención en las últimas líneas de esta ponencia se debe a querer dejar en el aire el mensaje de que el camino que queda por recorrer, por lo que respecta a la modernización de la Administración, es más largo que el ya recorrido.

Muchas gracias.

Cuarto Panel: "LA COOPERACIÓN INTERNACIONAL EN EL CIBERESPACIO"