

Perspectivas del grupo de trabajo de CC-DRIVER acerca de las campañas de concienciación

El grupo de trabajo policial de CC-DRIVER, cuyo objetivo es el intercambio entre las Fuerzas y Cuerpos de Seguridad (FFCCS) en la UE de experiencias y buenas prácticas, con un enfoque específico en la ciberdelincuencia, ha concluido su tercera edición. En el encuentro, organizado virtualmente por Policía Local de València el viernes 11 de junio, 7 cuerpos policiales de 5 países (Finlandia, Alemania, Grecia, Eslovenia y España) debatieron acerca de las mejores prácticas y lecciones aprendidas en las campañas de concienciación llevadas a cabo por las FFCCS.

Las campañas de concienciación persiguen el cambio en el comportamiento individual de acuerdo con las normas y actitudes sociales. Las FFCCS tienen un rol crucial en prevenir el cibercrimen mediante la concienciación. En la reunión se llegó a la conclusión de que las redes sociales constituyen un medio magnífico para acercar a las FFCCS a la ciudadanía, especialmente a la juventud. En los siguientes párrafos se analizan los principales temas debatidos durante el encuentro.

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) publicó el pasado mes de abril un informe a nivel europeo llamado [Cyber Security Month \(ECSM\) 2020 Deployment Report](#), en el cual se muestra que la participación en redes sociales se triplicó en 2020, en comparación a 2019. El grupo de trabajo policial de CC-DRIVER señaló varias buenas prácticas que podrían haber contribuido a este aumento. Por una parte, las acciones coordinadas y simultáneas aunando esfuerzos ante temas comunes tales como las estafas cibernéticas y las habilidades digitales, y los hashtags como #ThinkB4UClick, parecen haber ayudado a la hora de lograr estos buenos resultados. Por otra parte, la gran disponibilidad de materiales, la facilidad de descargar, imprimir y traducir los documentos a los 24 idiomas de los participantes, así como el uso de diferentes medios de comunicación, desempeñaron también un papel crucial.

La cuenta de Twitter de la Policía Nacional @Policia es la cuenta de perfil policial con más seguidores en todo el mundo (3,5 millones). Esto ha contribuido a mejorar su servicio público y a crear relaciones de confianza con la ciudadanía gracias a una comunicación bidireccional y dinámica. Este caso contrasta con un desafío habitual señalado por el grupo de trabajo: la falta de experiencia en este ámbito de profesionales gestores de redes sociales en los cuerpos policiales, debido a que los y las mejores se encuentran en el sector privado donde se ofrece una mayor remuneración. Todavía queda

mucho por mejorar en cuanto a las campañas de concienciación, ya que las personas especializadas en ciberseguridad en el sector público llevan a cabo normalmente las investigaciones en lugar de organizar campañas de concienciación y prevención.

En otro orden de cosas, también se mencionó el proyecto Medi@4sec, finalizado en 2018, y financiado por el programa H2020 de la UE. Este proyecto se centró en el uso de las redes sociales para fines de seguridad pública y, además, realizó un mapeo, disponible en su página web, de las mejores prácticas de las FFCCS en redes sociales a nivel global.

Durante el encuentro se debatió también sobre campañas orientadas a las víctimas como [«Say no!» de EUROPOL](#). Su objetivo es concienciar sobre la coerción y extorsión sexual online que afecta a menores. La mayoría de las campañas orientadas a víctimas llevadas a cabo por las FFCCS participantes se centraron en la protección de la juventud contra el cibercrimen y en los negocios contra el ransomware (cibersecuestro de datos). Se consideraron como buenas prácticas tanto el aumento en las recompensas para las víctimas como la publicidad de la reducción del riesgo.

En lo que concierne a las campañas orientadas a delincuentes llevadas a cabo por las FFCCS, el grupo de trabajo trató varios ejemplos y buenas prácticas. De nuevo, y como ejemplo de una campaña bien pensada, se trajo a colación la campaña de EUROPOL [«Cybercrime vs Cybersecurity: what will you choose?»](#). La policía finlandesa mencionó también un programa de intervención multidisciplinar que se está llevando a cabo con jóvenes ciberdelincuentes que ya han cometido ciberdelitos, o que podrían cometerlos en el futuro debido a sus intereses y conocimientos. Otras buenas prácticas fueron: anunciar mayores riesgos y reducir recompensas, centrarse en delitos y zonas geográficas específicas y presentar alternativas realistas y viables para las personas que delinquen.

Con respecto a la gestión de la información en redes sociales en escenarios donde el orden social y la seguridad pública están comprometidos, tales como ataques terroristas, Twitter ha demostrado ser una forma efectiva de contrarrestar rumores. En dichos escenarios, los perfiles de Twitter de las FFCCS deberían convertirse en una fuente de información rápida y de confianza. Ejemplos de esto son la policía de Múnich y los Mossos d'Escuadra, que gestionaron adecuadamente la información durante y después de un ataque terrorista. Además de ofrecer información rápida y actualizada, el desarrollo de una lista de verificación de comunicaciones, previa a dichos incidentes, es otra buena práctica que ha demostrado ser de gran importancia.

Por último, se concluyó que la ciberseguridad debía ser una responsabilidad compartida entre agentes públicos y privados, y las FFCCS del grupo de trabajo policial de CC-DRIVER dejaron claro que un intercambio de información debía tener lugar. Es un hecho que el sector privado no declara los ciberataques y/o puede que elimine las pruebas, convirtiéndose en un reto serio para las FFCCS en su lucha contra el cibercrimen. Por lo tanto, la mejora de los canales de cooperación y el fortalecimiento de las asociaciones público-privadas mejorarán la respuesta de los cuerpos policiales a este problema de creciente importancia