Relatoría Track
Ciberseguridad

Fecha: 13 de setiembre 2017

Descripción del panel

Para que Internet se convierta en un espacio inclusivo y que funcione como motor para la economía digital es necesario generar confianza en su uso mediante la implementación de políticas públicas, acciones de las empresas privadas y el desarrollo de capacidades de los usuarios. Es por ello que el debate se debe realizar atendiendo a la participación de todas las partes interesadas, definiendo qué se entiende por 'ciberseguridad', un término no exento de controversias. En la agenda nacional quedan temas pendientes como la adhesión al Convenio de Ciberseguridad de Budapest o la promulgación de una Ley de Delitos Informáticos.

Integrantes de la mesa
Eduardo Lima (Ministerio del Interior- Gobierno)
Carlos Martinez (LACNIC- Comunidad Técnica)
Santiago Paz (Certuy)
Martin Pecoy (Universidad de Montevideo- Academia)

Moderador/a
Beatriz Rodriguez. Internet Society Uruguay Chapter. Comunidad Técnica.

Relator/a
Paula Oteguy. LACNIC

Pregunta
Beatriz Rodriguez toma la palabra en primer lugar, agradeciendo a los panelistas y participantes. Luego indica que se tratarán temas de la vida cotidiana sobre ciberseguridad y que el propósito será lograr una noción de que podemos hacer al respecto. Para entender y comprender los temas presenta uno a uno a los panelistas quienes integran las diferentes partes interesadas.

Respuesta

Carlos Martinez toma la palabra en primer lugar. Agradece el poder compartir el segundo IGFUY. Comienza indicando que prefiere una visión menos académica de seguridad, en el sentido que la seguridad como tal y cuando uno usa Internet tenemos nuestras espectativas, como por ejemplo que nuestros datos están yendo hacia algún lugar seguro, pensando que nuestros datos no están siendo analizados en tránsito. Indica que esto son propiedades implícito donde todos esperamos que eso se cumpla, sin embargo explica que esto a veces falla y conspira contra la confianza del uso digital en las actividades del día a día. Seguido habla del concepto de Seguridad Colaborativa, donde todos tenemos un rol que cumplir, desde el operador hasta el usuario final. Indica que de todo lo que puede

ocurrir en el uso de Internet, a él le ha tocado la seguridad a nivel de infraestructura y protcolo, que es una parte pero se necesitan de todas las partes restantes.

Pregunta
¿Como podemos saber cual es la situación particular sobre ciberseguridad en Uruguay?

Respuesta
Santiago Paz, toma la palabra en segundo lugar y responde. Comienza indicando que a nivel Estado se utiliza un enfoque defensivo en lo que respecta a ciberseguridad y estrategia. Indica que el ecosistema de ciberseguridad en Uruguay fue desarrollado con marco normativo, institucional, capacidades técnicas, marco cooperativo y capacidades en general, también indica que está integrado por varios actores. Explica que para enfrentar problemas de ciberseguridad uno puede tener instalado su marco legal pero si no tiene el músculo para responder en tiempo y forma no servirá de nada. Realiza metáfora con un equipo de fútbol, diciendo que podés tener el mejor equipo pero si solo se le enseña el teórico a la hora de salir a jugar a la cancha no tendrán buen desempeño. Explica que desde AGESIC cuentan con centros de operaciones de ciberseguridad, los cuales mejoran la detención de los problemas, donde las 24hs hay una persona encargada de esto, pudiendo frente a incidentes responder en minutos, no en horas como sucedía antes. También cuenta que se empezó a probar tener en las instalaciones físicas, espacios para trabajo conjunto a nivel global y comenta que esta iniciativa está muy incorporada en otros países y que el objetivo es llevarlo a la práctica acá. Cuenta que han existido 800 incidentes al año, piensa que estos casos se multiplicarán por lo que para dar respuesta se necesita el trabajo en conjunto. Concluye con la idea que desde el gobierno se está trabajando en el desarrollo de capacidades operativas y trabajo en conjunto con todos los demás actores.

Pregunta
Beatriz expresa que la ciberseguridad va avanzando, afectando a todos, hasta actores que parecían invulnerables. Dirige la pregunta a Martín Pecoy: ¿Que pensás sobre esto?

Respuesta
Martín Pecoy, toma la palabra en tercer lugar. Comienza hablando de wanna cry, cuenta que un colega vió encriptada toda su notebook y que la solución fue pagar con bitcoins y salir rápidamente del problema, pero él pregunta: ¿es la solución?, responde que no es la recomendada, no es la solución recomendada en bases internacionles e indica que el Convenio de Budapest, viene a decir verdades sobre esto. Budapest presenta la mayor cantidad de recomendaciones globales, es un documento elaborado desde el año 1997 al 2001 con más de 30 borradores distintos, es un Convenio de mínimos pero con multiplicidad de formas de combatir delincuencia.
Budapest ha generado cultivo en Europa con pautas de procedimientos para combatir los comportamientos, si se lograba aplanar las fronteras de la persecución, se renovaba el delito a distancia, con la particularidad de que el ataque podía ser anónimo. Es decir que estaba en crisis la territorialidad del derecho penal, eso llevo a que se invitara a actores que no integraban la realidad europea, pero si eran países con fuerza, como EEUU y Japón, también se convoca Argentina, para que en la región sea un referente. Cuenta que existen países en contra del Convenio, que manifiestan que se debiera hacer o re redactar en el ámbito de Naciones Unidas, como Brasil y Rusia.

Frente a la cuestión de si tenemos o no posibilidad de seguir Budapest, tiene consecuencias, como es el caso de Brasil y Portugal, caso paradigmático, países semejantes pero con diferencias que evidencian las dos posturas de seguir o no Budapest. Brasil presenta distinción en cuanto a acceso ilícito porque Portugal presenta acceso ilícito, sin embargo Brasil dice que debe existir daño de datos o revelación de información confidencial.

También expresa que nos encontramos en la 3ra era de cibercrimen, comenzando por virus amateurs, luego delincuencia organizada, lo que hoy plantea consecuencias a nivel geopolítico. La Convención de Budapest puede ser una guía ya que sugiere nuve delitos específicos, se puede calificar protección de contenido, secreto, propiedad intelectual, en ese plano establece cierta base para la tipificación pero indica que el mayor contenido está dado en un aspecto procesal, donde las normas dentro del Convenio duplican el Derecho sustantivo, con esto tenemos una visión clara de la necesidad de un régimen jurídico que acompase desde el punto de vista de la persecución los mecanismos posibles a nivel procesal.

Finaliza hablando sobre la situacion en Uruguay donde desde el punto de vista penal existen tres proyectos de Ley que quieren seguir Budapest, pero ninguno consiguió estudio en el Parlamento. Comenta que AGESIC esta con revisión del proyecto 2014 para la consideración de creación de nuevas figuras. Agrega que si hemos cumplido con ciertos aspectos como el haber sido pioneros en delincuencia informática y falsificaciones informáticas. Desde el año 1996 contamos en Uruguay con una Ley de castigo de falsificación de documento electrónico**.**

Tenemos la esperanza de que se cuenten con las figuras típicas y necesarias, conocer que le esta pasando, el grado de victimización y para que sectores de la población, de no mirar esto seria derecho penal simbólico.

Pregunta

¿Como se procede en Uruguay ante el enfrentamiento con delincuentes?

Respuesta

Eduardo Lima, toma la palabra en cuarto lugar. Responde que desde el año 2005 se está trabajando sobre delitos informáticos, trabajando en conjunto con colegas del extranjero que capacitaron a los funcionarios locales, principalmente en temas de pornografía infantil.

Expresa que en lo referente a delito informático, a nivel policial se ven dos cosas: la tecnología como medio y la parte legal, el marco jurídico que lo contempla. Ante esto si bien el código contempla algunas áreas, a nivel de Uruguay estamos carentes en alguna tipificaciones específicas. Muchas veces se trabajan dos cosas a la vez, cuenta que se trabajan operación sobre mega estafa donde participan distintos países y a la vez casos de difamación social de red social, donde el Ministerio les ha dado las herramientas necesarias para investigar, pero lo que demora la aclaración del caso es la cooperación internacional de las empresas privadas.

En relación a los tipos de delitos en Uruguay cuenta que en los comienzos del año 2005 era mas sencillo sin embargo hoy en día con la deep web y servidores anónimos genera dificultades para ser rastreado. Lo que se da mas es fraude a los usuarios por medio de phishing o mensaje de texto. Afirma que todo es decepcionado y si bien no hay marco jurídico los casos son tomados en cuenta para analizar las nuevas tendencia.

Indica que a nivel de policía nacional, existe una unidad de crimen organizado en parte de delitos tecnológicos y se crea nueva unidad llamada departamento de informática y análisis web, la cual realiza las búsquedas en redes sociales sobre conductas delictivas, como estafas y difamación, entre otras, que se investigan y transmiten a la justicia, sin embargo indica que es complicado llegar a la instancia penal, pero afirma que de todos modos se generan informes a nivel nacional.
Finaliza indicando que en lo referente a los mecanismos legales, si bien el Código Penal contempla aspectos, no lo hace con todos. Por ejemplo la Ley de abuso sexual infantil, contempla el verbo almacenar, pero ante casos no se ha podido comprobar a la justicia que ese acto sea para difundir o intercambiar, sino que solamente era contenido almacenado, por o que la persona queda en libertad dado que el almacenaje aquí no es delito.

Pregunta del público 1
En España la visualización de pornografia infantil es delito sin embargo en Uruguay no lo es. ¿Existe alguna iniciativa para cuidar esto?

Respuesta
Eduardo Lima responde que se ha planteado la cuestión a raíz de distinta investigaciones, pero debe pasar a una etapa de legisladores, por lo que no depende de ellos. Aclara que el almacenamiento no es prueba porque no es delito, no hay nada que lo prohiba. Pone el ejemplo de que si alguna vez sabemos que alguien almacena ese tipo de información, no se estaría cometiendo delito, y más allá de lo moral, explica que si ese contenido existe es porque alguien lo requiere.
Pone un ejemplo práctico de trabajo en conjunto con Alemania, los que tenían años atrás equipos específicos donde se conectaban a las computadoras y solicitaban PTHC, sigla de referencia de pornografía infantil, estos le brindaban la IP del usuario, lo enviaban a Uruguay por INTERPOL pero aquí no se puede judicializar dado que como ya se expresó, el almacenamiento no es prueba porque no es delito. No hay algo que prohíba tener almacenado este tipo de información.

Pregunta del público 2
¿Cuál es la situación de Uruguay en base al relacionamiento con la justicia? ¿Consideran que en los últimos años el entendimiento mutuo ha mejorado, o debemos avanzar? ¿Contamos con las herramientas necesarias para la prueba?

Respuesta
Eduardo Lima expresa que siempre se debe avanzar, que han trabajado en conjunto con AGESIC y se ha investigado. Existen un equipo de fiscales del Ministerio para encautación y evidencia digital, que emepzará a regir a partir de noviembre de este año, contempla custodia y almacenamiento. En colaboración con los jueces se expone como se llegó al resultadod e la investigación, aportando toda la información, también los policias se apoyan en reclamos de abogados defensores, quienes defienden a los clientes y buscan los errores sobre ellos.

Martin Pecoy agrega que existe un problema de falta de colaboración. Si por ejemplo se pide información a Gmail, estos muchas veces no brindan respuesta, indica que la integración por parte de la policía puede ser una de las fuentes para la colaboración, pero aclara que cualquier de los actores privados deben cumplir con estándares en cuanto a conservación de datos, dado que algunos los eliminan en un mes.

Pregunta del público 3
¿Están dadas las condiciones de seguridad y legales para implementar mecanismos de participación ciudadana en la toma de decisiones?

Respuesta
Santiago Paz responde que en lo que refiere a participación ciudadana las condiciones tecnológicas están dadas. Pone como ejemplo la CI electrónica con niveles de seguridad extremadamente altos y tecnologías criptográficas, sin embargo apunta a que existen otras condiciones que hoy no son atendidas y hay que atenderlas, como por ejemplo el conocimiento en las personas.

Pregunta del público 4
Con 800 ciberataques al año, y en relación a que todo se reduce a conocer la IP proveniente del ataque, ¿esa cifra registrada de ciberataques proviene del medio nacional o extranjero?

Respuesta
Santiago Paz aclara que la cifra 800 es la que se arroja luego de identificado el incidente, luego de esta etapa se contabiliza en la cuenta, indica que no existe metodología global para medir. En lo que refiere a la dirección IP esta no es lo único pero es un dato importante, dice que existen técnicas, como Red Tor, que anonimiza a los usuarios y es complejo llegar al origen. Concluye diciendo que no es un tema que afecte solo a Uruguay sino a todo el mundo y explica que frente a un ataque en un país quizá el atacante no es de ese mismo país, expresa que pensar en geografía política en el ámbito de Internet es poco preciso, no existen límites geográficos.

Martín Pecoy agrega, en el mundo se dice que es cuestión de software, pero si se logra rastrear la serie de conexiones que taparon la original se puede llegar a lograr la dirección y ahí se vuelve crucial la colaboración que mencionamos desde el comienzo.

Carlos Martinez agrega que existen técnicas para disimular la IP pero ninguna es 100% perfecta, todas permiten un análisis para saber de donde provienen, explica que si pueden complejizar la investigación pero no es tan perfecto. Contó su experiencia años atrás en ANTEL, donde antes del 2005 actuando como testigo ante un caso de ciberatque era notorio que el juez efectuaba preguntas sin saber de que se estaba hablando, sin embargo a partir del año 2005 los informes y oficios de la policía reflejaban un entendimiento mayor de la materia, con esfuerzos conjuntos de las distintas partes interesadas. Hace incapié en que Internet está en un momento de cambio que tiene que ver con el agotamiento de las direcciones IPv4 y el despliegue de IPv6. Lo agrega como ejemplo paralelo pero situado en el año 2017 y explica que un juez enfrentado a este caso podría estar en una situación muy parecida a la del año 2005 donde no sabían como proceder, por lo que remarca la

importacia de transmitir y recabar la mayor cantidad de información posible, como por ejemplo, el puerto de orige que puede ser muy relevante.

Beatriz Rodriguez, moderadora del panel indica que el tiempo se ha cumplido, que sin duda es un tema muy interesante del cual debemos seguir conversando. Se da paso al siguiente panel.