Published on *Hoy en el TEC* (https://www.tec.ac.cr/hoyeneltec)

Roni Zehavi, director de CyberSpark, en la charla sobre ciudades inteligentes que impartió el miércoles 24 de mayo en el Steinvorth, San José. **Foto: OCM.**

Ciberseguridad y desarrollo tecnológico

‘La seguridad digital se debe empezar a enseñar desde las escuelas’: entrevista con experto internacional

5 de Junio 2017 Por: Johan Umaña Venegas [1]

Entrevista con el *CEO* de CyberSpark, un parque tecnológico israelí, líder mundial en materia de ciberseguridad

Roni Zehavi es el director ejecutivo de CyberSpark [2], una interesante y moderna iniciativa que combina los mejores aportes de la academia, la industria –con empresas insignes del sector, como IBM, Cisco y PayPal– y el gobierno de Israel, el país líder a nivel mundial en

materia de ciberseguridad.

Este experto visitó el país el pasado mes, invitado por la Embajada de Israel en Costa Rica, para brindar una serie de charlas sobre ciudades inteligentes, seguridad digital y varios temas relacionados.

También atendió a varios medios de comunicación, entre ellos ***Hoy en el TEC*** (el pasado 25 de mayo), para conversar sobre el desarrollo de CyberSpark, parque tecnológico dedicado a temas de seguridad digital desde la prevención de virus cibernéticos hasta lo que será la futura certificación de los automóviles inteligentes; las particularidades de esa alianza entre lo público, lo privado y lo académico; y, por supuesto, cómo mejorar la seguridad digital en nuestros hogares y organizaciones.

De sus enseñanzas, resalta su facilidad para explicar un tema tan complejo como la ciberseguridad, a la que **compara con la medicina cuando aduce que todas las personas deberíamos realizar acciones cotidianas para proteger nuestros equipos y redes, así como cuidamos de nuestra salud con actos tan simples como lavarse las manos y comer saludablemente.**

También, que los niños deberían aprender desde la escuela a no abrir archivos adjuntos en correos electrónicos de extraños, de la misma manera en que aprenden las normas básicas de higiene.

A continuación, una traducción de la entrevista:

¿Cómo funciona CyberSpark? y ¿cómo ha sido la experiencia de esta comunión entre universidad, entidades públicas y empresas privadas?

CyberSpark empezó con la universidad, así que la universidad es el ancla del ecosistema completo. Luego, la industria empezó a llegar porque quería aprovechar tanto los egresados de la universidad como la investigación.

Fue la primera universidad que realmente graduó doctorados de segundo nivel en ciberseguridad. Fue la primera a nivel mundial, ahora hay algunas más. No en ingeniería computacional o ciencias de la computación, hablo de ciberseguridad. Así que los egresados de esas facultades son muy valiosos para la industria y eso atrajo a las empresas.

El gobierno, que puso mucho énfasis en ciberseguridad, identificó estos campus como un gran capital de ciberseguridad en Israel, y empezó a trabajar en conjunto, como una compañía, que es CyberSpark y que está localizada entre la universidad, la industria y el gobierno, juntos.

La iniciativa trabaja muy bien, porque nos sentamos alrededor de la mesa y decidimos cuáles son todas las cosas que queremos hacer juntos, cómo la industria puede influenciar a la universidad, cómo la universidad puede ser más efectiva para la industria y cómo el gobierno facilita todo.

En Latinoamérica son incipientes las experiencias de alianzas entre la academia, la empresa privada y el ámbito público. Desde su experiencia, ¿cómo se impulsa este modelo? y ¿cuáles son las ventajas?

Primero que nada, el gobierno tiene un rol muy importante, de hecho está a cargo de varias cosas. Desarrollar capital humano es responsabilidad del gobierno, así que es muy útil que exista una entidad dedicada a la ciberseguridad dentro del gobierno, como ocurre en Israel y no en todos los países.

Ellos (el gobierno) proveen tanto incentivos fiscales para la industria, como inversión en centros de investigación junto a la universidad, y esto es muy útil.

> “Es muy positivo que los líderes del departamento de desarrollo e investigación en las grandes compañías estén involucrados en ajustar el perfil de salida (de los estudiantes) de la universidad; porque una cosa es que usted tenga profesores que te enseñen, pero si tienes además gente proveniente de IBM, de Cisco, de Intel...”

Después, es importante que los inversionistas tengan bastante experiencia en el mundo exterior, para que puedan identificar buenas ideas en la universidad y convertirlas en compañías de alta tecnología. Es muy positivo que los líderes del departamento de desarrollo e investigación en las grandes compañías estén involucrados en ajustar el perfil de salida (de los estudiantes) de la universidad; porque una cosa es que usted tenga profesores que te enseñen, pero si tienes además gente proveniente de IBM, de Cisco, de Intel..., de todas esas compañías que trabajan de cerca en el tema de ciberseguridad y saben cuáles son las necesidades del mercado, pueden ir a la universidad y asegurarse de que los graduados vayan a ser mucho más maduros en la materia.

¿Cuáles son los principales retos que enfrentó el desarrollo de CyberSpark?

Cada una de las distintas entidades, la universidad, las grandes compañías, las pequeñas compañías..., tienen sus intereses particulares y su propia agenda. La universidad está ahí para enseñar, para investigar y publicar *papers* (artículos científicos).

La industria está para generar dinero, para hacer negocios. Pero ninguna compañía, aunque las más grandes lo quieran, tiene la capacidad y la atención para abarcar el ecosistema completo. Así que CyberSpark es una iniciativa que ha sido nominada por todas esas entidades para encargarse de desarrollar este ecosistema, tanto internamente en Israel como en el extranjero, y asegurarse de que se haga bien.

¿Cómo se maneja el tema de patentes y propiedad intelectual en ese ambiente conjunto?

La propiedad intelectual no es manejada por CyberSpark. La propiedad intelectual es manejada, caso a caso, estudio a estudio; directamente entre la universidad y la industria. Así que si la universidad va a desarrollar algún estudio en conjunto con la industria, primero discuten entre ellos cómo lo van a hacer y cómo compartir la propiedad intelectual, dependiendo del porcentaje de equidad y la inversión de cada quien. Pero nosotros, como CyberSpark, no nos relacionamos

con eso.

Recientemente el tema de ciberseguridad ha tomado mucha preponderancia, con varios ataques masivos famosos. ¿En qué nivel de seguridad diría usted que nos ubicamos mundialmente? ¿Es la Internet muy vulnerable?

No creo que podamos responder la pregunta de qué tan vulnerables somos, porque es como preguntar qué tan vulnerable es la especie humana ante las enfermedades. Depende mucho de cada individuo. Usted puede estar muy bien protegido y yo puedo ser muy vulnerable.

La ciberseguridad está basada en varios aspectos, por ejemplo, uno de ellos es la ingeniería humana, así que al *hacker* que quiera atacar a una compañía u organización, o ministerio del gobierno, podría intentar enviar un *email* con un archivo adjunto. Si en la organización todos está bien informados, nadie abrirá ese archivo adjunto. y serán menos vulnerables.

> “Creo que, en general, si las personas se apegaran a lo básico, como cambiar sus contraseñas, no abrir archivos adjuntos, asegurarse de hacer las cosas correctas, no caer en la tentación de hacer cosas estúpidas, el nivel de vulnerabilidad será aceptable”

Así que es muy difícil contestar, creo que, en general, si las personas se apegaran a lo básico, como cambiar sus contraseñas, no abrir archivos adjuntos, asegurarse de hacer las cosas correctas, no caer en la tentación de hacer cosas estúpidas, el nivel de vulnerabilidad será aceptable. Aunque, a pesar de eso, todo es *hackeable*, es simplemente una cuestión de dinero y recursos y qué tan importante es. Depende, si se trata de un individuo que está muy molesto con alguna organización y la intentará hackear, es una cosa; si es un anarquista, es otra cosa. Pero si se trata de un gobierno, si el gobierno de Corea del Norte quisiera atacar algo, lo va a lograr atacar, porque va a tener a mil personas trabajando en eso y en mes y medio seguramente lo lograrán hackear.

Es muy difícil decir qué tan vulnerable está el Internet, es una combinación de muchas cosas para determinar el nivel de riesgo o la cantidad de protección.

Desde su experiencia, ¿cómo se pasa de ser un país reactivo a los ataques de ciberdelincuencia a ser proactivo?

Para llegar de la situación en la que ustedes están, de ser un país activo a ser un país proactivo, la clave es tener conciencia al respecto. Se ocupa esa conciencia y la motivación, a nivel nacional, para reconocer que se debe atender el tema de la ciberseguridad. El conocimiento está ahí y está basado en colaboración con otros países, como el caso de CiberSpark, en la educación y en el desarrollo de la industria de la ciberseguridad.

> “Se debe reconocer el problema y darle la importancia debida. Con solo esas dos cosas, un país puede pasar de activo a proactivo en temas de seguridad cibernética”.

Pero, primero se debe reconocer el problema y darle la importancia debida. Con solo esas dos

cosas, un país puede pasar de activo a proactivo en temas de seguridad cibernética.

¿Cuáles son las mejores prácticas que debería realizar un Gobierno para garantizar una adecuada ciberseguridad?

Lo primero es capital humano, definitivamente. A nivel nacional, el país tiene que identificar plenamente cuál es la brecha y cuánta gente capacitada en ciberseguridad necesita. No sé cuál es la respuesta para Costa Rica, pero digamos que ocupa 5.000 personas capacitadas, entonces la pregunta se vuelve "¿cómo preparar a esas 5.000 personas en tres, cuatro o cinco años?".

> "Se debe iniciar en las secundarias, creando conciencia en los estudiantes sobre qué es ciberseguridad, motivándolos para matricularse en carreras de este tipo".

Hay que empezar desde la secundaria, porque si empieza a nivel universitario ya es muy tarde. Se debe iniciar en las secundarias, creando conciencia en los estudiantes sobre qué es ciberseguridad, motivándolos para matricularse en carreras de este tipo.

La ciberseguridad es muy interesante, representa un gran reto y es multidisciplinaria. Por ejemplo, si alguien quiere ser un abogado, puede enfocarse en seguridad virtual, privacidad y ese tipo de cosas. Si las personas quieren estudiar filosofía, pues también hay muchas cuestiones en ciberseguridad relacionadas a la ética, privacidad, propiedad de las bases de datos, y otros. Así que en casi en toda disciplina uno puede encontrar una aplicación a la ciberseguridad. Así que hablamos de un campo que es retador, es bien pagado y es cambiante todo el tiempo. Si usted le dice eso a los estudiantes de secundaria, seguramente ellos pensarán que es un tema interesante y que les gustaría trabajar en algo relacionado, de forma que cuando ingresen a la universidad o busquen un posgrado lo tendrán en cuenta. De esa forma, habrá personal capacitado capaz de suplir las necesidades de la industria. Todo este proceso es responsabilidad del gobierno, que debe tener una visión a nivel nacional y destinar fondos para motivar estudios en ciberseguridad, También se debe invertir en centros de investigación, quizá en conjunto con la industria, lo que permitiría la participación de empresas como IBM, Cisco y otros.

Pero así es cómo se debe hacer, desde el sector gubernamental. Lo primero es desarrollar el capital humano.

¿Cuál es la mejor forma para educar a las personas en cuanto a la prevención?

Es similar a cuidar la salud. ¿Cuál es la mejor manera de enseñarle a la gente a ser saludables? ¿Cómo se puede acercar a las personas para hacerles notar la importancia de lo que comen, que hagan ejercicio y tomen otras medidas? Hay muchas maneras de acercarse a las personas y decirles "hay una amenaza, no se lo decimos para asustarle o intimidarle, porque hay muchas cosas que se pueden hacer, pero usted tiene que saber al respecto".

> "Así como los niños aprenden a lavarse las manos después de ir al baño y se ha vuelto algo común, algo que no era común hace 100 años pero que hoy en día todo

> el mundo lo hace... Es lo mismo con la ciberseguridad".

Así como los niños aprenden a lavarse las manos después de ir al baño y se ha vuelto algo común, algo que no era común hace 100 años pero que hoy en día todo el mundo lo hace... Es lo mismo con la ciberseguridad. Si usted le enseña a sus niños a no abrir un archivo adjunto cuando reciben un correo electrónico de alguien desconocido, es prevención. Así que es importante enseñarles desde la escuela, porque hoy en día desde tempranas edades ya se tiene acceso a celulares. Hay que enseñarles cuáles son las amenazas y cómo enfrentarlas.

> "Es común que las personas piensen que la ciberseguridad es una tarea propia de un técnico, un tema complicado que no comprenden. Pero yo le aseguro que usted está haciendo muchas cosas para mantenerse saludable sin que sea doctor y nunca estudió en una escuela de medicina".

Es común que las personas piensen que la ciberseguridad es una tarea propia de un técnico, un tema complicado que no comprenden. Pero yo le aseguro que usted está haciendo muchas cosas para mantenerse saludable sin que sea doctor y nunca estudió en una escuela de medicina pero sí sabe qué debe hacer para mantenerse saludable. Es exactamente lo mismo, es un cambio de perspectiva, pero es posible.

Más allá de la ciberseguridad, ¿cuál es el estado mundial respecto a legislación y acciones para procesar delitos cibernéticos?

Es un problema gigantesco, no nos alcanza el tiempo para discutirlo, pero es un problema muy importante. Si alguien irrumpe en su hogar, usted llama a la policía. Pero si alguien ingresa a su computadora no tiene mucho sentido acudir a la policía, porque ellos no van a hacer nada. Las leyes y las entidades que se encargan de hacerlas cumplir están muy atrasadas. Están intentando ponerse al día, pero es muy difícil, porque es difícil saber quién lo hizo, dónde está..., ya que la geografía no tiene nada que ver, el criminal puede estar en Corea del Norte y la víctima aquí en San José. Están intentando ponerse al día, pero no se pueden tomar en cuenta.

Usted hace alusión a que la manipulación de datos es el mayor riesgo informático de la actualidad y es virtualmente indetectable. ¿Qué tan grande es el riesgo en los sistemas actuales?

Si usted intenta *hackear* un aeropuerto y el aeropuerto cierra, no es muy conveniente, pero en general el mundo ha adoptado cosas como manejo de crisis para asegurarse la continuidad de los negocios. Así que el aeropuerto puede cerrar por un terremoto y ya existe un plan de contingencia para responder si eso pasa. Lo mismo pasa con robar dinero del banco, está asegurado y el banco sabe qué hacer para proteger el dinero.

> "El problema con la manipulación de datos es que nadie sabe que la información ha sido manipulada".

El problema con la manipulación de datos es que nadie sabe que la información ha sido manipulada. Piense en su sistema inmunológico, si su cuerpo es atacado por una bacteria, su

sistema inmunológico podrá reconocer que hay un problema y empezará a atacar a la bacteria. Las peores enfermedades son las autoinmunes, que es cuando el cuerpo se ataca a sí mismo y el sistema inmunológico no reconoce que existe un problema. Eso pasa con el cáncer, el cuerpo no reconoce que existe un problema.

Eso es lo que es la manipulación de datos. Nadie reconoce el problema, porque todo se ve normal, solo es un cambio de información. Toma más tiempo, pero los daños son gigantescos y esto es algo que se debe atender inmediatamente.

Enlaces
[1] https://www.tec.ac.cr/hoyeneltec/users/johan-umana-venegas
[2] http://cyberspark.org.il/affiliate-club/