One Hacker

Tim Grieveson, de HPE: "El nuevo reglamento europeo de datos es una gran oportunidad y lo hará todo más sencillo"

JOSÉ M. VERA Martes 18 de julio de 2017, 19:01h http://www.onemagazine.es/one-hacker-job-business-entrevista-ciberseguridad-hpe-isms-forum-2017?cache=true

Aprovechando su presencia en el foro del ISMS Forum Spain, Grieveson, uno de los grandes expertos ciber europeos charló con One hacker sobre los retos que plantean las nuevas tecnologías, el nuevo reglamento europeo de datos y su visión ante las nuevas ciber amenazas y cómo hacerlas frente.

Tim Grieveson es una de las referencias en ciberseguridad en Europa. Con más de 20 años trabajando en el mundo de la tecnología de la información y su protección, ahora trabaja para ofrecer herramientas a las empresas que permitan encarar su transformación digital de forma segura.

Aprovechando su presencia en el último foro del **ISMS Forum Spain** charló con **One Hacker**.

Dicen que el nuevo reglamento europe de datos lo cambia todo...

Puede hablar desde el punto de vista de HPE o tras haber sido CISO -responsable de ciberseguridad- pero creo que muchas empresas lo ven como una amenaza -por todos los procesos que hay que cambiar y cumplir- cuando debería ser una oportunidad para optimizar los costes y el negocio. Si entiendes los datos que tienes en el negocio, entenderás el valor de los datos y hace que ese proceso sea mucho mucho más simple. Además, si entiendes tu organización mejor, la tecnología y la seguridad estarán más integrados dentro del negocio desde un punto de vista de la gobernanza y la seguridad. Así que te será más fácil ver dónde hay valor y apostar por ello. Mucha gente sólo ve en el nuevo reglamento una obligación de invertir para evitar multas, pero conociendo mejor tus datos puedes pensar en nuevos mercados y proteger mejor tu empresa al saber dónde está su debilidad ante un posible ciberataque.

Qué tiene que cambiar en el mundo de la ciberseguridad de las empresas...

Tenemos que dejar de centrarnos en el endpoint -el terminal-, para mí lo importante son los datos. Vas a ser atacado., la brecha de seguridad ha pasado o pasará. El ransomware Cryptolocker, por ejemplo, causó pérdidas por un valor de 325 millones de dólares. Pero el atacante no obtuvo información de los datos que cifraba. Tú si puedes conseguir evitar pérdidas si apuestas por proteger bien los datos críticos para tu negocio. No trates de encriptar y protegerlos todos: te costará una fortuna y te llevará muchísimo tiempo. Para ello nosotros tenemos una tecnología, Format Preserving Encryption. Y lo mejor de ella es que no precisa archivos de gestión de claves enormes, ni disponer de un equipo de gente para gestionar certificados muy complejos. Así que es fácil de usar y permite que tercero usen los datos que ofreces de forma anonimizada para su negocio.

El gran desafío de la ciberseguridad...

Todo está en la nube. Así que uno de los grandes desafíos de la nube es su seguridad. Nuestro punto de vista es asignar la seguridad a los datos, respetar donde está en tu móvil, en tu ordenador, en la nube... y protegerlos. Así que, si alguien entra en la nube o en tu dispositivo obtendrá tus datos, pero no podrá usarlos de forma legible.

Y de las personas con el nuevo reglamento europeo de datos...

Va a hacer muchas empresas que pueden pasarlo mal si no protegen bien los datos de sus clientes. Incluso teniendo multas. La nueva normativa exigirá cambiar muchas cosas para garantizar el derecho al olvido de los individuos. También habrá más actividad criminal para intentar hacerse con datos personales. Y no sólo hay que temer una multa administrativa los daños reputacionales también pueden ser importantes. Incluso que puede haber operadores que pierdan su licencia por no haber protegido bien los datos personales de sus clientes. Ese es el gran impacto que puede ocurrir.

Así que en 2017 y 2018 será imprescindible...

Adaptarse a las exigencias de la nueva regulación para proteger los datos. Para ello también habrá que disponer de nuevas profesiones como la recien creada de Delegado de Protección de Datos (DPD). Conseguir esas capacidades es todo un desafío. Pero también pienso que el nuevo reglamento consigue una cosa muy positiva: unifica regulaciones y hace más simple para toda Europa la regulación de datos.

¿Qué va a pasar con el Brexit?

Lo primero que hay que tener en cuenta es que este reglamento tiene que ver con el control y gestión de los datos de ciudadanos europeos. Si eres una compañía estadounidense o de Medio Oriente, tienes que cumplirla tanto en el uso como en la transmisión y el almacenamiento de datos de ciudadanos europeos. Así que es bueno en lo que afecta a nuestra privacidad. Por eso creo que, en caso de que se produzca el Brexit, Reino Unido aplicará una 'copia' de este reglamento también para su territorio.

¿Qué te apasiona de la tecnología?

La tecnología hace la vida de la gente más sencilla. Siempre he estado interesado en la tecnología. Gracias a la tecnología la colaboración es mucho más fácil, por ejemplo, la tecnología de comunicación. Yo viajo mucho y puedo comunicarme con mis hijos y mi esposa, mucho más fácil que antes. Cuando viajo puedo conseguir información en la palma de mi mano, mi vuelo, mi viaje, mi hotel...

¿Cuál es la amenaza que más le preocupa dentro de un mundo conectado en cinco o diez años?

Históricamente, los chicos malos solían ir tras un trozo de información, robar mis credenciales de la tarjeta de crédito... ahora están robando y clonando bases de datos. Así que, durante un periodo de tiempo, puedo no saber que he sido vulnerado hasta, por ejemplo, seis meses después. Es muy peligroso porque pueden ver mi tarjeta de crédito, los datos de mi estilo de vida, mis registros de salud... pueden robar hasta mi identidad. Imagínate que te roban la identidad. Y en proteger eso estamos. No queremos que nadie pueda, por ejemplo, usar tus datos para extorsionarte. Es muy preocupante pero **el riesgo existe y hay que protegernos ante ello.**

¿Te comprarías un coche conectado?

Tengo una berlina de una marca germana. Creo que cada vez más gente apuesta por el coche conectado. Pero también que se tiene que hacer mucho en proteger los coches autónomos y conseguir que sean seguros. HPE está trabajando con la industria del automóvil y se están tomando la seguridad de forma muy seria. Si piensas en nuestra tecnología de encriptado para las comunicaciones de coches autónomos es un buen ejemplo. Hay que tener cuidado de dónde uso la tecnología, para qué y qué datos almacenan mis dispositivos. Hay que aceptar que nuestros datos van a estar en Internet sí o sí... pero tienen que estar de forma segura...

¿Un consejo para vivir ciber seguro?

"Piensa como los malos", es la mejor forma de evitar amenazas. Si entiendes a tu enemigo -y no es necesariamente una mala persona- podrás protegerte. Hay que tener en cuena que puede ser alguien que no esté informado, o no tenga formación y puede causar muchos daños de forma inconsciente. Por ejemplo, es importante preguntarse, para mi empresa ¿cuál serían los datos con mayor valor para los tipos malos? ¿Qué técnicas usaría para intentar robarlos? Hay que concienciar más a los empleados y los profesionales. Es clave. Y diseñar con la seguridad como punto de partida.