Universidad de Talca
Facultad de Ingeniería
Departamento de Ciencias de la Computación

Seguridad Informática

Ensayo 4

El humo flota y los tontos lo siguen

Erik Regla
eregla09@alumnos.utalca.cl

25 de mayo de 2020

Supongo que siempre que a alguien le pasa algo, llega una persona que te dice: "Pero si ya va a pasar, no es para tanto". La típica persona que intenta darte ánimos pero que en realidad no tiene sustancia en sus palabras, contenido en lo que habla ni intenciones en su discurso. Ahora, no siempre es algo que ocurre, muchas veces es sin malas intenciones, pero hay una brecha super grande entre vivir cosas y estar aconsejando. Esto ocurre no solo en las relaciones interpersonales, también en las de trabajo, cualquiera que tenga un mínimo de experiencia laboral sabe que al lado siempre hay alguien que le pagan por mover la boca y salpicar saliva prometiendo el cielo, el mar y la tierra.

Y precísamente ahí está el problema, las promesas rara vez se ejecutan y mucho menos en consultoría. Quizás lo más triste a nivel de país es que no es porque falte talento, si no simplemente porque preferimos callar lo malo y hacer todo a medias. Total, ¿Llegando a la meta todos ganamos cierto?. Para nosotros esto nos abre una veta enorme, la venta de la *ciber-resilencia* como algo real, tangible y absolutamente necesario en el día a día.

Ahora la veta es grande, porque esto de la ciber-resilencia es como el sexo adolescente. Todo el mundo habla de ello, nadie sabe en la práctica como funciona pero como todos piensan que todos lo hacen entonces proclaman que son parte de el. Tan simple se nota desentrañar este contexto que bajo la definición de Accenture[1] *"Un enfoque flexible para lograr una empresa que combine disciplinas de ciberseguridad, continuidad del negocio y resiliencia"* -oh, vamos a combinar resilencia usando resilencia, por si no encontraban que los chistes recursivos eran fomes, acá tienen un nuevo candidato- mientras que Deloitte[2] dice que *"Ser Resilient significa tener capacidad de recuperación y minimizar el impacto de los incidentes"*. Mejor ni hablar de la definición de la Revista Gerencia [3] que la define como *"La capacidad inherente de una organización, entidad o Estado, que le permite enfrentar un ciberataque, sin que su negocio, función e integridad, se vean mayormente afectadas"*.

Entonces, ¿A quién le creemos? Podemos seguir todo el día buscando y vamos a seguir encon-

[1] https://www.accenture.com/cl-es/insights/cyber-security-index
[2] https://www2.deloitte.com/cl/es/pages/risk/solutions/ciber-resiliencia.html
[3] http://www.emb.cl/gerencia/articulo.mvc?xid=4647&ni=ciber-resilencia-el-estado-del-arte-para-enfrentar-los-ciberataques-y-el-cibercrimen-organizado

trando definiciones diferentes. El primer problema que tenemos que la ciber resilencia como tal no existe, es solo un concepto "marketero" que se usa para vender humo, el segundo es que es acuñado por personas que en realidad no tienen idea de lo que significa. Total, mientras el humo te lo venda una empresa reconocida, es de calidad.

Ahora, bien es sabido que una persona con talento puede incluso tomar humo y hacer un cuchillo afilado con este[4] asi que vamos a comenzar a aterrizar esto por conceptos.

Usualmente ciber -en realidad cyber- es típicamente utilizado para amenazas de seguridad en general. De ahi desprenden montones de términos, como cyberops que hace referencia a operaciones en general. No vamos a poner en discusión en este punto -porque se asume que el lector sabe ya- de por qué la seguridad es necesaria. Por otro lado resilencia, es un término utilizado en psicología para indicar la resistencia a situaciones adversas sin que haya una alteración importante del psique.

Esto último es importante porque en realidad cuando suele ocurrir un desastre, la primera reacción usualmente no es la mejor. Recuerdo cuando tuve mi primer incidente -que me pasó por ignorante en ese tiempo- y de no ser porque estaba acompañado de otras personas que ya tenían mas rodaje, la verdad no habría salido vivo. Por ejemplo, imagina que tienes un servidor con una interfaz directa saliendo a internet y de pronto el programa que tienes corriendo (asumamos un servicio en PHP de hace 10 años y nada puedes hacer porque tu empresa te obliga a usarlo) comienza a presentar problemas de tráfico.

Llegas a tu puesto de trabajo y lo primero que encuentras es que el sitio está sirviendo adware por todos lados. Esto claramente está mal, pero como algo sabes de infraestructura y que tienes que versionar tu trabajo cada cierto tiempo, te das cuenta que no es tarde para recargar una version de respaldo de tu base de datos, de tu aplicación y hacer un redeploy de la máquina porque usaste terraform. Entonces tienes dos alternativas:

- ¿Inicias el respaldo?
- ¿Le dices a tu jefe?

Si eres de los que elegiste la primera entonces fuiste víctima de la selección natural de la misma manera que la gente que abandona la ciudad en cuarentena. Estás haciendo perder al negocio mucho más que el día de desfase del respaldo. Estás perdiendo encontrar la fuente del problema, quizás hasta parchar una vulnerabilidad crítica en ese sistema de 10 años de antiguedad, los datos de clientes probablemente una demanda por fuga de datos. Mucha gente suele tomar la primera como la alternativa correcta, pero no se dan cuenta que en realidad solo realizan más daño.

Ahora si estás en un lugar relativamente serio te puedes tomar esto con algo mas de calma -que además se la merece-, si eres una persona seria entonces vas a aislar el componente afectado para examinarlo mas tarde y lo antes posible levantas un servicio secundario, al mismo tiempo que revisas el afectado para poder así parchar lo que haya salido mal. Utilizas esa información para elevar información a tu jefe porque al final el fue quien impuso la utilización de ese software, etc, etc. No es tan mala esa opción al final del día, ¿Cierto?

[4] ロウソクの黒煙を集めて作った包丁 - https://www.youtube.com/watch?v=zUCEMjhsvaU

Si llevamos la ciber-resilencia a su concepto más puro, entonces sería habilitar las condiciones para que los incidentes puedan ser resueltos con la seriedad que merecen. Una gran ventaja de ver este concepto en su estado puro es la promesa de poder rescatar lo mejor de situaciones donde la información es vulnerada, de poder entregar por medio de un plan concreto de acciones una propuesta de valor al cliente que también pueda dar tranquilidad.

Y esto no se logra contratando una empresa, utilizando el último antivirus o instalando firewalls hasta en las terminales clientes. Solo es posible lograrlo con educación, a nivel general para así subir la barrera del eslabón mas débil, implementando una estructura que de confianza en el uso de canales efectivos de comunicacion a los desarrolladores con sus jefes directos para poder informar de los problemas y estos puedan llegar a buen puerto. Una cultura proactiva de no esperar a que el incidente ocurra para resolver problemas de los sistemas y donde la seguridad no sea algo que se contrata luego de que ya es imposible hacer algo si no sea un conjunto de prácticas que entreguen confianza sobre el "sistema".

Pero esto último es demasiado para las empresas Chilenas, donde tenemos la cultura de poner a cargo a personas que nulo conocimiento tienen del cargo que desempeñan pero llegan gracias a su red de contactos, donde incluso una empresa de telecomunicaciones de importancia nacional designa a un encargado de seguridad es un ingeniero comercial. Esta es una de las desventajas operacionales mas grandes de implementar este concepto, la necesidad de ejecutar transformaciones que *sacudirán el arbolito*[5] para dejar caer esos adornos que no tienen función alguna.

Por eso, la ciber-resilencia que en realidad no es más que seguir buenas prácticas no es más que uno de esos terminos que utilizan "los comerciales" para poder vender más humo, cuando en realidad todos podríamos ser parte activa de esta.

[5] https://webpack.js.org/guides/tree-shaking/