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

Seguridad Informática

Informe 1

Dem charla

Erik Regla
eregla09@alumnos.utalca.cl

31 de mayo de 2020

Antes de abrir el informe -que en realidad es mas un ensayo-, quisiera aclarar que actualmente trabajo principalmente en RD y mi memoria es de investigación, por tanto la premisa de contrastarlo con algo que estoy haciendo o vaya a hacer, no aplica en mi caso. Sin embargo, me gustaría contrastar esto contra trabajos previos en los que he participado y una que otra aberración que he encontrado en el camino.

Uno de los temas tratados fue la relación casi de ficción que tienen la mirada las personas sobre la seguridad informática. Ahora, una mención especial a haber indicado la serie *Mr. Robot* como un claro ejemplo de esto, ya que en muchos lugares esta visión de la seguridad informática no solo es parte de clientes o de personas externas. Algo bastante común es que al momento de escuchar la palabra seguridad informática, son los mismos gerentes que piensan que esto es así.

Hace un tiempo atrás en alguno de esos lugares por los cuales pasé -por respeto al lugar no lo menciono pero con un poco de ingeniería social podrían hacerse una idea-, luego de un evento desafortunado donde se robaron los equipos y nadie estuviera haciendo nada más al respecto que llamar a la PDI, me tocó ir donde el gerente general para explicarle la situación y sus posibles implicancias (como por ejemplo que el robo general era para encubrir el robo de información específica de un cliente).

En ese momento claro, el gerente se comenzó a tomar en serio el tema de la seguridad, sin embargo, el problema constante para poder trabajar el asunto en los meses posteriores fue precísamente el dinero y la complejidad imaginaria del mismo. La visión expuésta por Nelson es bastante real, sin embargo, incluso si uno *parte por la cabeza de los problemas*, muchas veces las trabas vienen impuestas por factores culturales de la organización, no tomando cartas en el asunto hasta que no se materializa el riesgo como tal. Estas actitudes ponen en riesgo todos los aspectos de la seguridad, e incluso más, ponen en riesgo la reputación y la vida de la empresa en si.

Un segundo punto importante -que en realidad está dicho entre líneas- es que mantener un sistema de gestión de la seguridad tampoco tiene que ser algo extremadamente complejo, como tener que ejecutar pentestings como en las películas, haciendo todo desde cero y lanzando líneas de código a diestra y siniestra. De hecho existen muchas herramientas de fácil uso las cuales implementan

ya los análisis estándar como Nessus[1], las cuales ejecutan periódicamente assetments para poder verificar el estado de una determinada infraestructura expuesta u otros serivicios como los provistos por ZeroFox Platform [2] que se encargan de velar por detectar y evitar la fuga de información en las empresas por medio de la vigilancia social -otra forma de decirle a la ingeniería social- para detectar cuando ocurren o bien para poder prevenir estos en caso que se detecte que están siendo atacados por medio de redes sociales.

Si, todas estas soluciones requieren dinero, sin embargo ahi es donde está el tradeoff. Por lo general -al igual que en el caso anterior- la seguridad es de esas cosas que nunca se les da el peso hasta que no ocurre algún incidente, lo cual, al momento de vender este tipo de iniciativas es una buena idea poner los números en la mesa de costo/beneficio pero también los números de que implica un riesgo materializado como tal. Ejecutar un levantamiento para diseñar políticas o para la descripción de los activos informáticos de la empresa es crucial al momento de presentar este tipo de iniciativas.

Finalmente, como un tercer tema -que también está entre líneas- es el reconocer que el eslabón más debil es el humano. Hay cosas que ocurren de manera orgánica, por ejemplo, que un trabajador salga de su trabajo y migre a otro. Muchas veces cuando una empresa levanta a un trabajador no necesariamente es porque esté calificado, también uno de los factores que llevan a este levantamiento es el conocimiento adquirido en su anterior trabajo y como este puede beneficiar al nuevo lugar. Es por esto que muchos contratos tienen cláusulas de confidencialidad y cláusulas de contrato -que suelen decir que no te puedes ir a un lugar que haga algo parecido o a una competencia directa- justamente para prevenir fugas de información.

Sin embargo, un fenómeno bastante común en empresas pequeñas es la centralidad de la información por lo general dada por los miembros más antiguos. Recuerdo en algún momento haber visto un DBA -administrador de bases de datos- que es probablemente la persona con la que más discusiones he tenido en un trabajo. Como administrador de bases de datos no tengo reparos, probablemente para el trabajo especializado que hacía era uno de los mejores que he visto, pero el problema principal derivado por este mismo es que no documentaba ni soltaba los proyectos que tenía. Llegó a tal punto que habían proyectos cuya infraestructura era un castillo de naipes y era imposible repararlos o bien corregirlos porque todos estos proyectos dependían de una sola persona.

De parte de la gerencia no había mayor acción para corregir este problema, ellos solo veían que al momento de trabajar en un proyecto y era necesario involucrar a este DBA, entonces había que considerar el que debido a su carga sería un cuello de botella. A quien le pregunten en la empresa, la razón para poder hacer eso -no documentar, trabajar desordenado, generar arquitecturas frágiles o incomprensibles- no tiene otra mas que estar apernado al puesto. Dentro de la gerencia un par de voces estaban advocando por el hecho de cortar el problema de raiz asumiendo lo que implica el despido, asumiendo el costo en tiempo y el esfuerzo, pero utilizar esa oportunidad para re-estructurar las cosas. Pero nuevamente, el costo de que un proyecto se se pierda es mucho mayor a el costo que tiene su re-estructuración.

Ahora, en lo personal dos temas que me llamaron la atención fue en primer lugar el problema que genera que futuros profesionales del área de TI no tengan conocimiento alguno de UNIX. El

[1] https://www.tenable.com/products/nessus
[2] https://www.zerofox.com/

segundo es el tema de la firma digital, el cual personalmente siento que ha sido motivo de una venta de humo bastante grande. Por un lado tenemos lo propuesto por Nelson del uso de llaves criptográficas para la verificación de identidad, lo cual es algo extremadamente plausible y útil. En especial ahora en el contexo de la pandemia donde tienes que reducir el nivel de interacción persona-persona al mínimo y en lo posible habilitar el desarrollo de trámites personales directamente desde la casa para así prevenir contagios.

Sin embargo, también hay un numero importante de personas y desarrolladores que se llenan la boca con el blockchain como alternativa para transacciones seguras cuando en realidad ese no es el punto de su implementación. Tenemos casos emblemáticos como los que proponen cada 5 minutos usarlo para posibles elecciones donde el componente de la confidencialidad es extremadamente importante, cuando dejan de lado un factor de disponibilidad que es que solo puedan votar las personas que tengan que hacerlo. Por lo general y en mi opinión sincera algo que siento que es una regla de oro al momento de una auditoría es la facilidad de comprensión de un sistema como tal. Si un sistema no es auditable y comprensible por la totalidad de sus usuarios es una caja negra la cual no tiene forma de garantizar la confiabilidad de sus datos.