LA CONCIENCIA COMO PARTE IMPORTANTE DE LA GESTIÓN DE LA SEGURIDAD

Jorge Iván Morales, e-mail: jorgemendy28@hotmail.com
Noviembre 2015

***Abstract*—**In this document they will be are displayed a brief of actually of human awareness into a security systems. Which are the problems with this situation on small, medium and bigger corporations and how we could contribute to a fix it that situation through education and capacitation.

***Resumen*—**En este documento se mostrará un breve resumen de la actualidad de la conciencia humana entorno a la seguridad de los sistemas. Identificar cuáles son los problemas que esto acarrea en pequeñas, medianas y grandes empresas y de qué forma podemos contribuir para mejorar dicha situación a través de educación y capacitación.

***Palabras clave*—** Seguridad, humanas, comportamiento, hacking, personalidad, educación, capacitación.

1. INTRODUCCIÓN

Cada día la gestión de la seguridad toma un papel más importante en la realidad de todas las compañías sin importar su tamaño o su naturaleza, cada vez se tiene más en cuenta los riesgos asociados a un ataque informático y debido a que la seguridad debe ser transversal a la totalidad de las áreas de las compañías la conciencia en seguridad toma una relevancia importante ya que no basta con tener una infraestructura segura también es importante tener trabajadores consientes de los riesgos asociados a sus actividades laborales. También se debe tener en cuenta que la ingeniería social se ha convertido en una de las actividades preferidas por los atacantes, esta sugiere el aprovecharse de las vulnerabilidades humanas con el fin de obtener información que pueda ser de utilidad para mejorar la probabilidad de éxito de un ataque informático. Existen múltiples técnicas que facilitan a un atacante realizar ingeniería social todas ellas representan tanta facilidad como mayor sea el desconocimiento del trabajador o atacado.

2. ANTECEDENTES

En cualquier organización el número de personas encargadas de asegurar la información de la compañía es muy bajo con respecto al número total de empleados por tanto la seguridad debe ser una tarea de todas las personas que intervienen en un proceso. Uno de los problemas más graves que afectan a las compañías es la fuga de información, según Symantec en su reporte anual de 2013 dice que este fue el año de las «megafugas». El número de fugas de datos (253) fue un 62% más alto que en 2012, y también se superó el total de 2011 (208). Sin embargo, estos datos no bastan para entender la gravedad del problema. Lo verdaderamente preocupante es que ocho de las fugas que se produjeron en 2013 dejaron al descubierto más de diez millones de identidades cada una. En 2012, solo hubo un incidente de esa magnitud, y en 2011, la cifra llegó solo a cinco. En todo el año, quedaron 552 millones de identidades expuestas y se pusieron

en peligro los datos personales relacionados con ellas (Direcciones, contraseñas, datos de tarjetas de crédito, etc.). [1] Estas cifras realmente son alarmantes, pero más preocupante aún es considerar las causas de estas fugas de información.

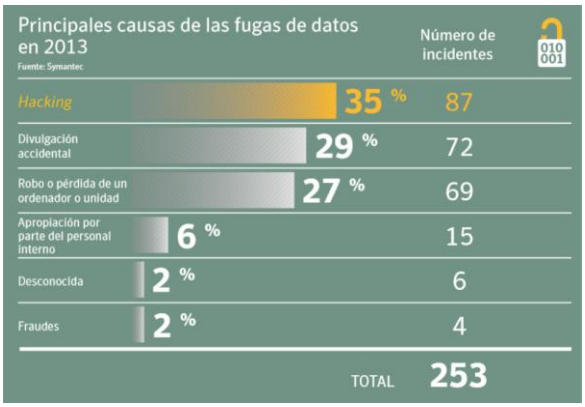

Figura 1 Causas de fuga de información [1]

Si nos detenemos a revisar cuidadosamente la gráfica anterior se puede evidenciar que el 35% de las fugas de información corresponde a hacking el cual se basa en aprovecharse de las vulnerabilidades de los activos informáticos, sin embargo el 29% corresponde a la divulgación accidental de información la cual puede corresponder a un desconocimiento de los riesgos por parte de las personas, en tercer lugar se encuentra el robo o pérdida de un ordenador o unidad de almacenamiento lo cual a mi juicio también podría evitarse o mitigarse con conciencia en la seguridad por lo anterior se podría inferir que un 56% de los casos de fuga de información están sujetos a remediación mediante buenas campañas educativas.

3. PROBLEMA

Según PCI Uno de los mayores riesgos para la seguridad de la información de una organización a menudo no es una debilidad en la tecnología. Más bien, es la acción o inacción de los empleados y demás personal que puede llevar a los incidentes de seguridad, por ejemplo, a través de la divulgación de la información que podría ser utilizado en un ataque de ingeniería social, no informar de la actividad inusual observada, el acceso a la información sensible no relacionada con la función del usuario sin seguir los procedimientos apropiados, y así sucesivamente. Por tanto, es vital que las organizaciones tengan un programa de concienciación sobre la seguridad en el lugar para asegurar que los empleados son conscientes de la importancia de proteger la información confidencial, lo que deben hacer para manejar información de forma segura, y los riesgos de un mal manejo de la información. Comprensión de los empleados de las consecuencias organizativas y personales de mal manejo de información sensible esto es crucial para el éxito de una organización. Algunas consecuencias del mal manejo de la información pueden llegar a ser hasta Sanciones impuestas contra la organización, el daño a la reputación de la organización y los empleados, y el impacto que el trabajo de un empleado. Es importante poner el daño potencial de la organización en perspectiva para el personal, que detalla cómo esos daños a la organización puede afectar a sus propios roles. [2]

Actualmente se ciernen muchos inconvenientes de seguridad para las compañías sin importar su tamaño o naturaleza, dichos problemas sugieren riesgos enormes por tanto pensar en seguridad se convirtió en una prioridad en las empresas, la seguridad debe ser una cadena compuesta por varios factores (infraestructura, procesos, recurso humano etc.) y las cadenas son tan fuertes como su eslabón más débil, se dice que el eslabón más débil en la cadena de la seguridad es el ser humano, y a menudo este factor no es ampliamente visualizado ni tenido en cuenta. Generalmente se piensa que con una infraestructura de seguridad es suficiente pero tal como se vio en los antecedentes mencionados en este documento las personas y sus falencias personales pueden acarrear el mismo riesgo que tener infraestructuras no aseguradas. Las personas pueden ser influenciables, sus acciones y comportamiento

pueden ir en contra de la seguridad de la compañía facilitando la materialización de los riesgos antes expuestos.

Algunos de los factores importantes del ser humano que pueden ir en contravía de la seguridad son:

- Inexperiencia

Este factor es de gran importancia y se presenta en las personas cuando no cuentan con la ductilidad para manejar los sistemas de información, esto puede ocasionar errores que a su vez se desencadenan en riesgos sobre la confidencialidad o integridad de los datos de la compañía. También se podría presentar cuando se contrata una persona nueva y maneja información sensible sin la adecuada capacitación.

- Personalidad

Mucho antes de que las personas ingresen a trabajar a una compañía han desarrollado una serie de comportamientos asociados a su personalidad y a menudo estos comportamientos involuntariamente peligrosos pueden desencadenar fuga de información sensible que puede ser usada por una entidad maliciosa para hacer daño de alguna forma a la compañía afectándola de manera grave.

- Entorno Social

Las compañías no se encuentran en la capacidad de evaluar o juzgar el entorno de uno de sus trabajadores, sin embargo este entorno puede llevar a un ser humano a querer obtener beneficio de alguna información que se encuentre a su alcance siempre motivado por alguna tercera persona que pueda tener fines económicos o de diferentes factores con esta información.

- Intereses económicos

Tal como el entorno social puede influir negativamente en un trabajador para cometer ilícitos relacionados con la información también se puede presentar intereses personales del trabajador que conociendo la importancia y sensibilidad de la información que maneja quiera sacar provecho de ella.

Los mencionados anteriormente y muchos otros factores son los causantes de que el ser humano sea el eslabón más débil de la cadena y uno de los blancos preferidos por los atacantes para sus actividades maliciosas, sin embargo existen algunas actividades que se pueden realizar con el fin de mitigar la exposición al riesgo del ser humano.

4. MÉTODO DE ACCIÓN

En definitiva la conciencia de seguridad está ganando un papel fundamental en la lucha contra las falencias que puede contener el ser humano y que se convierten en riesgos asociados a la seguridad informática. Como primera medida se debe garantizar que la seguridad en las compañías tenga el balance perfecto de tal forma que las políticas de seguridad no compliquen las funciones diarias de las personas ya que esto podría provocar una apatía de parte de los trabajadores.

Se debe motivar el uso correcto de los activos de la compañía y de esta forma garantizar que se obtenga el mejor provecho de la infraestructura y por ende se haga de forma segura.

Sensibilizar a los usuarios al respecto de la seguridad puede ser una buena estrategia para lograr el objetivo de blindar la compañía de riesgos humanos, quizás realizando actividades que igualen los riesgos personales a los riesgos laborales.

La conciencia de seguridad debe llevarse a cabo como un programa permanente para garantizar que la formación y el conocimiento no sólo se entregan como una actividad anual, sino que se utiliza para mantener un alto nivel de conciencia de seguridad diariamente. [2]

Una conciencia de seguridad basada en roles proporciona a las organizaciones una referencia para la formación de personal en los niveles adecuados en función de sus funciones de

trabajo. La formación se puede ampliar, combinar o disminuir según los niveles de responsabilidad y las funciones definidas en la organización. El objetivo es construir un catálogo de referencia de diversos tipos y profundidades de capacitación para ayudar a las organizaciones a ofrecer la formación adecuada a las personas adecuadas en el momento adecuado. Si lo hace, va a mejorar la seguridad de la organización. [2]

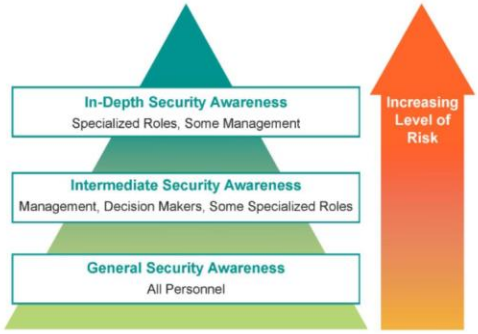

Figura 2 Entrenamientos de seguridad [2]

Conocer sus actividades y los riesgos asociados a ellas puede mejorar notablemente el entendimiento de seguridad de los empleados de una compañía repercutiendo esto directamente en la seguridad general de la compañía y ayudando a mantener los riesgos en niveles aceptables.

Como se ha mencionado en varias oportunidades durante el presente documento gestionar riesgos no solo hace referencia a la infraestructura tecnológica o a la información por sí misma. También se refiere al factor humano y sus vulnerabilidades, hacerlo de la mejor forma ya que no existen parches o firewall que se puedan implementar a los seres humanos y cada persona es un mundo con comportamientos y entornos diferentes y por lo tanto con vulnerabilidades y un factor de exposición al riesgo diferente.

Las políticas, procesos y procedimientos de una empresa enmarcan todas las capas de seguridad que se puedan tener en una empresa, estas políticas articulan todos los elementos presentes dentro de una compañía, y se debe tener muy en cuenta la socialización y sensibilización de dichas políticas dentro del personal de la compañía, esto también se realiza mediante capacitación y concientización.

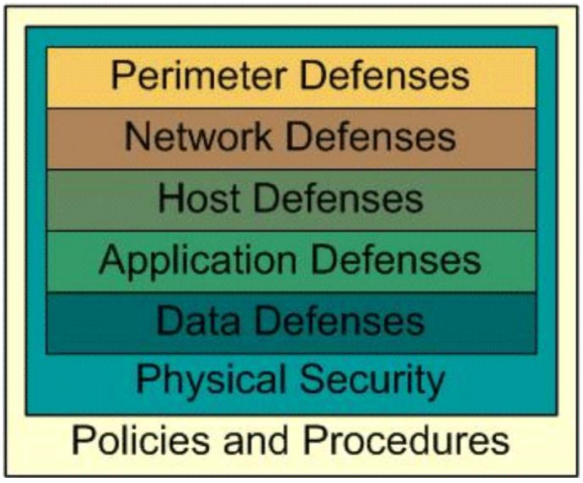

Figura 3 Capas de seguridad [3]

5. CONCLUSIONES

- Existe una serie de riesgos de seguridad asociados al factor humano los cuales a menudo no son tenidos en cuenta por las compañías.

- Las vulnerabilidades humanas son altamente aprovechadas por atacantes lo cual convierte a los empleados de una compañía en un riesgo latente si estos no cuentan con el conocimiento adecuado.

- Diversos factores del ser humano ajenos a la compañía pueden aumentar el factor de exposición causando posibles ataques informáticos.

- Las capacitaciones y educación asociadas a la seguridad y riesgos pueden disminuir las más comunes vulnerabilidades humanas mejorando la seguridad de una compañía a través de sus trabajadores.

- El dinero o esfuerzo asociado a una campaña de concientización se puede ver como una inversión ya que mejorará notablemente el conocimiento de seguridad de los empleados y por consiguiente la compañía mitigará los riesgos asociados a los trabajadores y al factor humano.

- La ingeniería social corresponde a la actividad a la cual el ser humano es más vulnerable en materia de ataque informáticos, estas técnicas tienen mejores resultados cuando los blancos de los ataques no están correctamente enterados o capacitados en las herramientas o información que ellos manejan lo cual los convierte en los activos más vulnerables

6. REFERENCIAS

[1] Certisur (2013). Informe de amenazas de seguridad Symantec 2013 [Online]. Disponible en: https://www.certisur.com/sites/default/files/docs/symantec-wstr-2014-cala.pdf

[2] PCI (2014) Best Practices for Implementing a Security Awareness Program [Online]. Disponible en: https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

[3] Ilinnois.gov (2013) Security Awareness for servers administrators [Online]. Disponible en: https://www.illinois.gov/bccs/services/catalog/security/assessments/Documents/security_awareness_server_admins.pdf