LA INSEGURIDAD INFORMÁTICA EN EL AMBITO SOCIAL

Gonzalez, Jairo
Universidad Piloto de Colombia

Resumen – La seguridad informática ya se ha convertido en un tema de manejo diario en la vida cotidiana de toda persona, no importando si tiene directa relación con los sistemas o no; en este momento todos los individuos poseen información valiosa no solo para ellos mismos sino para organizaciones o inclusive para comunidades enteras. En el momento se trabaja por varios vanguardistas de este tema sobre los conceptos de dualidad y de "Mente Segura" que permiten una mejor adaptación a los conceptos de seguridad que se trabajan en estos momentos.

Índice de Términos – Dualidad de seguridad, Proyecciones de seguridad, Mente Segura

I. INTRODUCCIÓN:

EN LA SOCIEDAD AL TERMINAR UN PERIODO Y COMENZAR EL siguiente, se presentan todos los resultados del anterior y se realizan unos pronósticos para poder prepararse para el siguiente. La seguridad informática no es diferente, es más, se vuelve un problema donde los especialistas en esta área trabajan para establecer estrategias y planes de acción

En la historia, algunos de esos pronósticos en el 2004 en seguridad [1] encontramos que temas como: el spam, los firewalls, los dispositivos de almacenamiento USB, las organizaciones criminales en internet, las regulaciones generan muchos cambios que afectan positiva y/o negativamente. Con estas ideas planteadas se desarrolla este breve documento donde revisamos el concepto de inseguridad informática desde una perspectiva social para comprender los elementos, relaciones y efectos de la seguridad informática en el ambiente de una sociedad siempre cambiante y dinámica e inesperada de la dinámica entre la tecnología, la organización y los individuos.

II. LA DUALIDAD:

El señor Jeimy Cano, en sus artículos considera: "El tema de la seguridad informática como una disciplina del conocimiento donde se busca cerrar la brecha de los eventos inesperados que puedan comprometer los activos de una organización y así contar con estrategias para avanzar ante cualquier eventualidad[2] El profesor Alexander Romero Coy explica a la seguridad como: "un estado de cualquier tipo de información (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo"[3] con estas dos explicaciones podemos validar como es que la seguridad informática, además de cambiar y ser dinámica en cuanto a las nuevas relaciones que explicaba Jeimy Cano, como a los estándares y normativas que son necesarias para aplicar todo lo relacionado (no solo a un sistema informático) sino también a la sociedad en sí.

En este sentido, se debería plantear la necesidad de revisar nuestra manera de abordar el tema de la protección de los

activos de una organización, no solamente establecer las causas y los efectos, sino comprender las relaciones entre los objetos revisados y considerar las reacciones entre ellas que pueden sugerir efectos que no puedan ser predecibles en los modelos actuales.

Al revisar la inseguridad informática como estrategia de pensamiento estratégico reconocemos que un sistema es tan seguro como su falla de seguridad más reciente, que cuando ocurre o se manifiesta un problema de seguridad las personas se vuelven más experimentadas y saben que hacer, que los sistemas mal diseñados (pensamiento natural en seguridad informática) no están preparados para fallar (pensamiento dual en inseguridad informática). En pocas palabras, mantener a tus amigos cerca, pero más cerca de tus enemigos.

La inseguridad informática como pensamiento dual en seguridad informática descubre que las relaciones entre los elementos del sistema son capaces de producir efectos positivos y negativos, los cuales son capaces de comprometer su supervivencia. En este sentido, comprender la inseguridad informática como el dual de la seguridad informática, en el contexto organizacional, representada esta última en sus participantes, sus procesos y tecnología (1) [CANO 2004], nos permite revisar las propiedades emergentes de la seguridad informática en un escenario con múltiples variables, repensar la seguridad misma más allá de una directriz de la corporación, como una mente pensante que aprende y evoluciona en su hacer.

III. MENTE SEGURA

Tratar las organizaciones como “mente segura” - Jeimy Cano indica en otro trabajo como interpretar todas las organizaciones como un solo individuo y nos introduce en un concepto de “mente segura” en base a la evolución que se ha vivido en cuanto a la seguridad. En este punto quiero hacer énfasis en la situación cuando no existe seguridad; que se hace necesario una evaluación de comportamientos, procedimientos, políticas, reglas y controles para poder determinar un nivel óptimo de seguridad al menos en un mediano o corto plazo de las situaciones que pueden ser vulnerables o riesgosas. El porqué de esto es para considerar que sin estos elementos nuestra organización se puede volver una “mente insegura” y ser susceptible y atractiva a ataques severos.

En este orden de ideas es como campos del conocimiento como la criptografía, aplicaciones automatizadas y diseño de hardware más seguro toman fuerza en distintas organizaciones; en esto podemos ver el ejemplo de las fuerzas militares, que cada vez se capacitan más en protección de la información, dando especial cuidado a estas áreas. Donde la seguridad de las naciones se basa en la información automatizada.

Pero el concepto de mente segura no es el manejo de las instituciones militares de la información, pero si es basada en ello. Para describir mejor esto, tenemos que ver como se manejaba la seguridad informática en los años 90; donde se popularizo la Internet y aparece el nuevo concepto de seguridad distribuida. Donde la seguridad informática ya no dependía tanto de un equipo, sino también en la seguridad de la interacción, la seguridad

de las relaciones humanas que ya se generaban en ese mundo. Y de ahí nacieron los primeros estándares. [4]

Sin embargo, como lo explica Jeimy Cano [5] *()* se puede ver como se habla de una reconciliación y no una incorporación como tal, a finales de los 90 muchas organizaciones no habían interiorizado en sus esquemas el concepto de seguridad en sus procedimientos, inclusive hoy en día se puede evidenciar como los ataques son por falta de preparación en los procedimientos de acuerdo a estas prácticas seguras.

Pero esto está cambiando, ya corporaciones e individuos están implementando prácticas (individuales o corporativas dependiendo). En organizaciones ya se encuentran modelos de seguridad aceptados y avalados por estándares internacionales. Se ve como la visión se está transformando hacia esa protección que antes no vigilaban con la premura necesaria.

Prácticas en Seguridad – Estas prácticas se basan en tres agentes: La tecnología (T) La organización (O) y el individuo (I) y en base a sus interacciones, las cuales permiten evaluar y diagnosticar las fallas, así poder definir planes y concentrar acciones específicas.

Ya identificando las tres partes, se define una tabla resumen de los riesgos que existen (Tabla No 1) en ella se aplica una X en la parte donde el riesgo está asociado. Esta asociación puede ser por parte de procedimientos, herramientas o conocimiento.

El principal objetivo de esta tabla es poder definir como se afectan los diferentes procesos con el TOI, en base a eso se pueden organizar responsabilidades y generar análisis.

Practicas	***Organización***	***Tecnología***	***Individuo***
Validación de fortaleza/debilidad de contraseñas	x	x	
Pruebas de penetración (Internas/Externas)		x	
Control de acceso vía contraseñas (estáticas/dinámicas)		x	
Uso y actualización de sistemas antivirus	x	x	
Definición y uso de registros de auditoría en sistemas electrónicos e informáticos		x	
Clasificación de la información corporativa	x		
Análisis de riesgos y controles sobre la información	x		

Tabla No 1
Cuadro Resumen

En este ejemplo se puede determinar con claridad que la mayoría de temas de la seguridad informática sobre tecnología, esto indicaría que las herramientas de

seguridad corresponden a recursos de la parte de tecnología, y a su vez, dependiendo esta de la alta gerencia.

Además, en el campo individuo se denota la falta de relación entre estos dos temas, y se denota uno de los puntos más débiles, y por lo tanto, más atacados en la actualidad; el usuario se convierte en el objetivo más utilizado para vulnerar un sistema de seguridad, y todo ello derivado a una falta de preparación, herramientas y capacitación por parte de los lineamientos actuales.

En el momento existen algunas prácticas seguras que integran al individuo en sus esquemas, con buenas practicas, mayor conocimiento de herramientas de seguridad e invitando a la reflexión en los conceptos de seguridad; pero para ello es necesario evaluar y rediseñar los conceptos del TOI.

Pero entonces ¿cómo se puede pensar en "Mente Segura" con todos los vacíos existentes? Para ello el ingeniero Jeimy Cano plantea estas directivas:

i. La seguridad debe ser una consideración diaria
ii. La seguridad debe ser un esfuerzo comunitario
iii. Las prácticas de seguridad debe mantener un foco generalizado
iv. Las prácticas de seguridad deben incluir algunas medidas de entrenamiento para todo el personal de la organización

Cada una de estas directrices busca (como se dijo anteriormente en este artículo) relacionar más al individuo con la seguridad informática y no ser tratado como dos temas tan diferentes o distantes. Si se logra interiorizar estos conceptos a todo individuo, apalancado en una disciplina y la conciencia corporativa.

Las 8 reglas de la seguridad informática – Además de las 4 directrices, el ingeniero Jeimy Cano postula 8 reglas de la seguridad informática:

i. Regla del menor privilegio
ii. Regla de los cambios
iii. Regla de la confianza
iv. Regla del eslabón más débil
v. Regla de separación
vi. Regla de los tres procesos
vii. Regla de la acción preventiva
viii. Regla de la respuesta apropiada

Regla del menor privilegio: se otorga el acceso para la labor solicitada exclusivamente.

Regla de los cambios: Los cambios deben ser coordinados, administrados y considerados en función de las implicaciones.

Regla de la confianza: Se debe comprender los efectos de dar nuestra confianza a un tercero.

Regla del eslabón más débil: Un sistema es tan fuerte como lo es su componente más débil.

Regla de separación: Para mantener un elemento seguro, se debe separar de elementos inseguros.

Regla de los tres procesos: La seguridad no termina en la implementación; también necesita de monitoreo y mantenimiento continuo

Regla de la acción preventiva: Alerta sobre una seguridad efectiva sin una adecuada preparación preventiva.

Regla de la respuesta apropiada: Lo importante de tener en claro las acciones a ejecutar ante un incidente de seguridad

IV. CONCLUSIONES

En el actual mundo, todavía quedan muchas fallas; sin embargo, estas mismas fallas permiten que todos los esquemas de seguridad se vayan fortaleciendo. Es interesante el concepto que se maneja en la dualidad, donde para que un sistema se vuelva más robusto y confiable, tiene que ser atacado varias veces.

La seguridad informática ha tenido una clara y fuerte influencia en el medio tecnológico, lo que al principio se creía que solo expertos en esta área eran los encargados de manipular y comprender, además de ser los únicos responsables, de todos los temas de seguridad.

Ahora se está demostrando que debe ser por vía de un manejo más integral, donde todos los implicados (procesos,

Se demuestra cómo es necesario entonces la inseguridad para volvernos más expertos en el tema de protección y prevención, y cuando más nuevos riesgos aparecen, y así, toma su debida importancia.

REFERENCIAS

[1] GREGORY, P. 2003, SAVAGE, M. 2003

[2] CANO, JEIMY, "Dualidad de la seguridad Informática"

[3] ROMERO, ALEXANDER *http://alexromeroc.blogspot.com/*

[4] Ashton Security Laboratories, http://www.ashtonlabs.com/rainbow.html

[5] CANO, JEIMY "un concepto extendido de la mente segura: pensamiento sistémico en seguridad informática"