Mesa de Moderación. Congreso Iglesia y cultura digital, Chile
Entendiendo las inseguridades de la información
Omar Villota Hurtado © 2011

1. La información es el activo más importante de la actual Organización del siglo 21. La divulgación de dicha información utiliza, en principio, las tecnologías de información y telecomunicación; esto es internet como red de arquitectura abierta y las tecnologías de comunicación móvil que permiten que cualquiera se pueda localizar en cualquier lugar y proveer, desde allí, al mundo entero.
2. No obstante, se observa empíricamente lo contrario. La industria proveedora de contenidos más la tecnología de Internet se han concentrado fundamentalmente en las principales áreas metropolitanas de los principales países del mundo. La razón es muy sencilla: precisamente porque la tecnología permite localizarse y distribuir desde cualquier parte, lo esencial para producir contenido en Internet es tener información y conocimiento, lo que se traduce en personas con esa información y ese conocimiento, que están sobre todo concentradas en los grandes centros culturales y grandes áreas metropolitanas del mundo.
3. Desde la perspectiva histórica, el conocimiento en red ha desplazado, primero, la fuerza muscular humana, y ahora las máquinas mecánicas. Implica entonces que los modos de circulación del saber han experimentado una mutación: en el momento es disperso y fragmentado, escapa de los lugares que antes lo contenían y legitimaban, dejó de pertenecer a figuras sociales que lo detentaban y administraban.
4. Este supuesto trabajo colaborativo de gestionar conocimiento en red es decir, descentralizado alberga proyectos colectivos, desde la comunicación y la educación, esquivando la mirada crítica sobre la aceptada “verdad” posmoderna de la información. No se habla de los asuntos excluidos por las multinacionales, que lejos de nivelar el juego de la globalización con empleos y tecnología para todo el mundo, imponen a los países más pobres salarios mal pagados y en pésimas condiciones de seguridad social. Esta es otra de las inseguridades de la industria tecnológica.
5. La transmisión libre y simultánea de contenidos digitales recibidos en aparatos de telecomunicación ubicuos no garantiza un modelo de red democrática, que podríamos considerarla como “aquella que defiende a los más optimistas desde un modelo horizontal, libre y desterrritorializado, o como un sistema sin centro donde cada nodo puede operar como un todo autónomo dificultando tanto la destrucción como el control de la propia red”.
6. Existe en la pragmática otro modelo de red autoritaria caracterizado por los sistemas de difusión. Esta es la inseguridad al conocimiento extendido, libre, compartido. La red de transmisión se caracteriza por su producción centralizada, por su distribución masiva y por su comunicación en un solo sentido: escasean los autores con alfabetizaciones digital y multimedial. Es decir, solo 2 mil millones de 7 mil millones de personas en el mundo utilizan las llamadas TIC. Aun cuando, usar no es sinónimo de emplear ni emplear es igual a aprovechar. Otra inseguridad que se agrega son nuestros 488 millones de 910 millones de conciudadanos americanos al interior de las tecnologías. Y se seguimos bajando en la escala, está muy lejos la democracia de la red en Colombia, donde escasamente 14 millones de 46 millones de compatriotas mal contados hacen uso de las TIC.
7. Evitar vulnerabilidades en la industria de la seguridad de la información es establecer un esquema de gestión de seguridad de la información, que se transforma en una búsqueda de patrones y posibilidades para reconocer la dinámica de la inseguridad informática. Lo que permite alcanzar mayores niveles de confiabilidad, no de seguridad. Ante esta vulnerabilidad que abre paso a la inseguridad de la información, la industria vende dos distinciones, la del tema de productos y servicios, y la de buenas prácticas, listas de chequeo y estándares.
8. Gestionar la inseguridad informática desde la vulnerabilidad significa conjugar la dinámica de la industria de la seguridad, la renovación constante de las vulnerabilidades del software y la psicología del individuo. En consecuencia, se sugiere que dicha recomendación debe ser una iniciativa para descubrir y comprender algunas de las relaciones que se materializan al evidenciarse una falla de seguridad.
9. La psicología de la seguridad de la información implica desarrollar y ejecutar nuevas y mejores decisiones con base en el análisis de incidentes de pérdidas de datos. La seguridad es una sensación en los niveles del riesgo cuya teoría dice “a medida que las personas se sienten más seguras con medidas de seguridad, se vuelven más propensas a los riesgos”.

10. El mercado incluye diferentes formas de vender seguridad de la información pero estas prácticas deben pasar primero por un filtro de evaluación de necesidades propias de la organización, la comprensión clara de la dinámica del negocio y las limitaciones propias de los productos. Algunas estrategias vendidas por la industria de la seguridad de la información:
    - Explotación del miedo y de la incertidumbre para crear la sensación de que estamos en el filo del abismo: una adecuada administración de riesgos y una cultura de seguridad organizacional nos permiten mitigar y manejar la exposición natural a las vulnerabilidades propias de la tecnología.
    - Exposición a intrusos de productos de seguridad de la información para que intenten quebrarlos y cuando no lo hacen, la industria los proclama con la leyenda publicitaria "imposibles de hackear": someterse al escrutinio de terceros es una buena estrategia, pero requiere un alto nivel de participación y calidad de los evaluadores del producto.
    - Ofrecimiento al proveedor de una visibilidad en el mercado de productos y servicios consumidos por una compañía específica o una entidad del gobierno: lo mejor es contactar directamente a la organización que los adopta para conocer en detalle el tema de contratación y uso de la misma.
    - Evaluación en revistas populares de la industria de servicios y productos: esta forma de mercadear el producto promociona no el resultado mismo de la evaluación sino el haber sido seleccionado como uno de los productos reconocidos en el mercado, y lo hace acreedor de prestigio.
    - Establecimiento y recomendación de los proveedores y de organizaciones internacionales de listas de chequeo, certificaciones de negocio y modelos de control que procuran salvaguardar a las organizaciones de los más importantes peligros en temas de seguridad de la información: muchos de los resultados de estos estudios internos muestran tendencias de la realidad que deben ser consideradas al interior de cada organización y no apreciadas como estudios formales con investigación rigurosa.
    - Generalizar "buenas prácticas" junto a productos y servicios para su distribución empresarial: representan lo que la industria y la práctica sugieren que es lo más adecuado sin considerar las diferencias entre compañías y negocios frente a sus necesidades particulares.
11. El costo de la inseguridad en el software y en las aplicaciones, y cómo los ataques a estos elementos son parte de la problemática ¿qué factores contribuyen a un crecimiento explosivo y exponencial de los ataques?
    - La velocidad en las comunicaciones es prosperidad y quiebra: incrementar la velocidad facilita que la organización llegue de inmediato hasta sus clientes pero también, que de manera rápida y eficiente, fluyan diversos métodos para fraudes o robos. Esta afirmación refuerza que la inversión en seguridad informática es inversamente proporcional a los datos.
    - La cantidad de dinero que gana en un mes ocupa sólo unos segundos: los incentivos financieros de rápido crecimiento y con mínimos esfuerzos a través de redes de telecomunicación atraen ganancias ilícitas incrementadas día a día. Existen redes de dinero en forma electrónica susceptibles de fallas y asaltos y nuestro laxo comportamiento ante cajeros electrónicos o telemáticos ayuda a la susceptibilidad para el desfalco y el asalto.
    - El volumen de vulnerabilidades reportadas en el software: los atacantes emplean un sin fin de formas para explotar y vulnerar los sistemas, desde aplicaciones corporativas como Oracle hasta computadores de casa como Apple OS X y Windows. Este factor requiere de aseguramientos de calidad en el software adquirido, de usuarios que reporten eventos de extraños, de aprender sobre el funcionamiento normal de los dispositivos, aplicativos y recursos.
    - Las soluciones de seguridad para proteger el software de ciberataques: la configuración y el afinamiento permanente de mecanismos de seguridad –particularmente los firewalls-, exige complejidad propia del software y conocimiento de las interacciones para mantenerlo funcionando adecuadamente. Si el usuario las desconoce debe llamar a un experto para evitar los riesgos.
    - La falta de coordinación transnacional de los agentes gubernamentales para tratar el tema del delito informático: si por lo menos dos naciones no comparten acuerdos sobre control, persecución y judicialización en los temas del crimen informático, los atacantes seguirán activos. Tanto abogados como juristas deben avanzar en la era del *Cumplimiento Electrónico*, que implica comprender los riesgos derivados del cruce entre tecnología, ley y mercado, como una manera de profundizar en las normas para englobar el delito informático y las relaciones entre el mundo offline y el online.

Bibliografía

Rice, David (2008). Geekonomics. The real cost of insecure software. Editor Addison Wesley.
Shostack, Adam y Stewart, Andrew (2008). The New School of Information Security. Editor Addison Wesley.
Cole, E. (2002). Hackers beware. Defending your network from the wiley hacker. New Riders.
Day, K. (2003). Inside the security mind. Making the tough decisions. Prentice Hall.
Horton, M y mugge, C. (2003). Hacknotes. Network Security Portable Reference. McGraw Hill.
Schneier, B. (2003). Beyond Fear. Thinking Sensibly about security in an uncertain world. Copernicus Books.
Whittaker, J. (2003). How to break software. A practical guide to testing. Addison Wesley.