Seguridad Informática de las empresas modernas

Enrique Daltabuit

La convergencia de las aplicaciones administrativas, de seguridad física, control de instalaciones, telefonía y manufactura complica la concepción de los procesos de seguridad y los métodos convencionales no son suficientes.

A mediados del siglo XX hicieron su aparición las computadoras en el mundo empresarial. También en esa época para satisfacer otros requerimientos, como la seguridad física y la manipulación del entorno de trabajo, se empezaron a usar sistemas cada vez mas sofisticados. El uso del teléfono se extendió prácticamente a todo el personal. Los procesos en manufactura se automatizaron. La combinación de estos sucesos dio origen a las empresas modernas. Muy pocas empresas funcionaban a mediados de siglo de la misma manera que a principios de siglo.

Paradoja de la productividad

Las ilusiones de que el uso de computadoras llevaría a las instituciones a trabajar en formas más eficientes, reduciendo su personal y logrando grandes avances administrativos perdieron su encanto. Las inversiones cuantiosísimas hechas en tecnologías de la información no se plasmaron en resultados concretos y cuantificables. Empezaba a propagarse un desencanto. Cobró fuerza la paradoja de la productividad enunciada como: "Entre más se invierte en tecnologías de la información menos resultados se obtienen" [1]

Hacia finales del siglo pasado John Burdette Gage y Scott McNealy, de Sun Microsystems, difundieron su paradigma "la red es la computadora". [10] Su empresa fue líder en la implementación de ese paradigma basado en la tecnología desarrollada por la agencia de investigación avanzada del ejército norteamericano (DARPA) y por la fundación nacional de investigación (NSF a través de NSFNET) que dio origen a Internet. A través de las tecnologías de la in-

formación y comunicaciones (TIC) ya no se requerían computadoras enormes para llevar a cabo los cálculos y procesos empresariales: las redes ofrecían a todo el mundo acceso a computadoras súper masivas y en paralelo. [12]

Internet

Cuando se logró que las computadoras se intercomunicaran y compartieran información la productividad aumentó, y la inversión que se había realizado rindió frutos, se ha producido un cambio radical en el funcionamiento las oficinas. Al principio se usaban las computadoras para cálculos científicos y militares, luego para cálculos empresariales tales como:

Administración
Contabilidad
Inventarios
Proceso de textos
Transacciones
Comunicación
Redes locales para compartir recursos
Almacenamiento masivo

Cuando NSFNET empezó a costar más de 100 millones de dólares al año, el Congreso norteamericano tuvo que forzar a que la administración de la red se licitara, y se admitieran empresas comerciales a la red (el llamado dominio.com). Entonces Internet se convirtió en una red que da servicio a todo tipo de instituciones. Se define Internet como una colección (inmensa) de redes que usan Ethernet y TCP/IP. [7]

La información de tipo administrativo que se encontraba en transito y en reposo en esta colección de computadoras estaba en alto riesgo. Los protocolos empleados no fueron diseñados para preservar la seguridad de la información. Las empresas buscaron emplear una solución que les permitiera aprovechar la tecnología disponible en forma estrictamente local y bajo su propio control.

Intranet

Pronto se desarrolló la tecnología de las Intranets, que son redes privadas aisladas que usan las empresas internamente para aprovechar las TIC que son el estándar a escala global, y luego la tecnología de los cortafuegos para conectar las Intranet a la red mundial.

Eso dio origen al acopio y minería de datos, tanto internos como externos. Estas colecciones de datos han resultado valiosísimas, dando la demostración de que la paradoja de la productividad era sólo la consecuencia de la falta de conectividad.

Esto requiere un cambio radical en las organizaciones pues la información primordial para su funcionamiento, no sólo administrativo u operativo sino táctico y estratégico, ahora requiere

del uso de redes privadas y públicas. Es indispensable fortalecer los procesos de seguridad proteger, tal como lo hacen los gobiernos, la información táctica y estratégica se ha logrado, aunque sólo en forma parcial.

A raíz de este funcionamiento fue necesario desarrollar una disciplina, llamada seguridad de la información, que se ocupa de la protección de los datos que se usan mediante esta combinación de redes privadas y públicas.

Convergencia

Pero además la misma infraestructura de TIC se ha empezado a usar para:
La seguridad física
La telefonía
El control de instalaciones
La manufactura

Que todas estas actividades compartan los recursos de telecomunicaciones provoca problemas. El funcionamiento armónico y simultáneo, ó sea la interoperabilidad, de los distintos sistemas que comparten recursos, impone condiciones sobre el funcionamiento de cada uno. Al integrarse dos sistemas el funcionamiento correcto de uno puede depender del funcionamiento del otro.

Según la ASIS (American Society for Industrial Security) [2] la convergencia de seguridad es " la identificación de los riesgos de seguridad y la interdependencia entre las actividades de negocios y los demás procesos dentro de una organización, y el desarrollo de soluciones institucionales para enfrentar los riesgos y las interdependencias.

Hay que distinguir entre:

- Interoperabilidad: dos sistemas muy distintos pueden intercambiar información o meta información pero siguen siendo independientes y llevan a cabo funciones separadas.
- Integración: dos sistemas comparten o reutilizan componentes y pueden depender el uno del otro, pero siguen realizando funciones separadas.
- Convergencia: Todas las operaciones y procesos comunes se llevan a cabo mediante un solo sistema.

Lograr la convergencia de las TIC en una empresa requiere un cambio en la estructura su funcionamiento para considerar congruentemente todos sus aspectos.

Choque de Culturas

Seguridad Física

La seguridad física se ocupa de la protección de los activos de una organización. El mundo de la seguridad física antecede por siglos a las TIC, y los encargados se dedican a proteger los activos físicos usando cerraduras, sistemas de vigilancia y sistemas de alarmas. Las personas encargadas de la seguridad física están entrenadas en

prevención de crímenes y en investigaciones policíacas. Es difícil que acepten la tecnología de seguridad informática que se ha desarrollado en los últimos 50 años para proteger la información. Por otra parte los responsables de las redes corporativas de datos no han sido capacitados en las estructuras de proyección de las instalaciones y las personas, situación que lleva a un choque cultural entre estos dos grupos. [9]

Seguridad de la Infraestructura
A mediados del siglo pasado los sistemas críticos se operaban manualmente aunque su supervisión estaba automatizada. A finales de ese siglo los sistemas críticos se operaban y se supervisaban mediante sistemas computarizados que estaban aislados, pero actualmente la mayor parte emplean conexiones basadas en los protocolos TCP/IP y forman parte de las redes institucionales (corporativas, institucionales o gubernamentales). Muchos de estos sistemas están completamente automatizados, pues las reacciones de los supervisores y operadores humanos son demasiado lentas, y los sistemas son sumamente complicados.

Hasta hace podo tiempo estos sistemas se usaban en forma reactiva para localizar fallas, almacenar datos operativos y llevar bitácoras de eventos para su análisis posterior. Las demandas de eficiencia han obligado a rediseñar los sistemas de control para darles funciones de administración que sirven para prevenir problemas, en lugar de sólo detectarlos y registrarlos. Tal rediseño generó arquitecturas de seguridad deficientes pues sólo se tomaron en cuenta criterios de productividad, confiabilidad y eficiencia operativa. Las tecnologías para proteger los activos se describen en el estándar ISA SP-90. [6]

Seguridad de la manufactura
Las empresas de manufactura usaban redes separadas para monitorear y controlar:

- el funcionamiento del negocio
- el funcionamiento de sus plantas

A lo largo de los años estas redes han sido diseñadas para transportar flujos de información distintos y tienen requerimientos de control distintos. Las redes corporativas que se usan para las funciones administrativas tradicionales y las aplicaciones como las de recursos humanos, contabilidad y adquisiciones están basadas en el protocolo Ethernet. [11]

Estas redes no se diseñaron con una arquitectura funcional o empresarial común. Puesto que la eficiencia, la fiabilidad y la rentabilidad dependen generalmente de algunas de estas capacidades, los fabricantes han implantado distintos tipos de redes que no se comunican entre si por ello la mayor

parte de las redes de manufactura se caracterizan por estar constituidas por muchas redes especializadas y generalmente incompatibles que coexisten en un solo espacio. [4]

Telefonía
usando el Protocolo Internet

La expansión explosiva del uso de Internet y de las TIC que ha aparecido en las empresas ha afectado también el universo de la telefonía. Como consecuencia muchas empresas telefónicas ya transportan su tráfico de voz usando la tecnología llamada "voz sobre IP" (VoIP). Una gran cantidad de empresas están aprovechando la flexibilidad de esta tecnología, así como el ahorro de recursos que implica el compartir los mismos medios físicos para transportar datos y voz.

Los teléfonos que habilitan VoIP comparten el flujo de paquetes en una red con los paquetes de datos y de otros tipos. Por consiguiente el tráfico de VoIP está sujeto a los mismos ataques a seguridad que el de datos. Hay también formas de emplear VoIP en redes inalámbricas, aceptando los riesgos adicionales que acompañan a este tipo de redes; basta con que un elemento de la red local en la que se encuentra el teléfono remitente de la llamada, o en la que se encuentra el destinatario de la llamada, o quizás algún punto intermedio, funcione en modo promiscuo para que todos los paquetes que constituyen la comunicación sean interceptados. [8]

Conclusiones

Este uso compartido de los recursos de las tecnologías de la información y de las telecomunicaciones obliga a que las empresas modernas organicen su administración de la seguridad de una manera más amplia. Al coexistir sistemas de seguridad de la información que se basan en políticas y concepciones diferentes, con prioridades diferentes, hay que tratar de evitar que en las interfases se creen problemas de seguridad adicionales.

Una causa fundamental de la inseguridad de la información radica en esta convergencia de funciones y tecnologías. Se origina en los conflictos culturales que se dan entre los responsables del manejo de los distintos tipos de información. En las empresas modernas hay que analizar, planear e implantar las redes convergentes tomando en cuenta los distintos procesos y sus características. Hay pues que plantear de inicio los procesos de la seguridad convergente.

Como se indica en la figura 1, la dirección general de la empresa tiene que emitir normas y buenas prácticas sobre los aspectos de funcionamiento de la empresa que afectan la seguridad de los datos. Las diferentes áreas administrativas que se responsabilizan de los distintos tipos de datos deben

interactuar con la dirección general en la elaboración de estas políticas y buenas prácticas. En la disciplina de la seguridad de la información se ha desarrollado diversas metodologías s para llevar a cabo este proceso, pero son numerosas y todas ellas complejas por ello dado el espacio disponible no se mencionarán

Figura 1

Referencias

[1] Atkinson, R. D. and Court, R. H. , (1998), Explaining The Productivity Paradox, The Progressive Policy Institute, THE NEW ECONOMY INDEX: http://www.neweconomyindex.org/productivity.html (verificado 12/03/08)

[2] Booz, Allen, Hamilton, (2005) Convergence of Enterprise Security Organizations, The Alliance for Enterprise Security Risk Management http://www.asisonline.org/newsroom/alliance.pdf

[3] Carlson, R. Burgess A. Miller. C, (1996),Timeline of Computing History ,Computer : IEEE Computer Society, http://csdl2.computer.org/dl/mags/co/1996/10/rxTL1.pdf (verificado 12/03/08)

[4] Caro, D.,(2004), Automation Network Selection, Instrumentation Society of America.

[5] Gampati, V., (2005), Convergence of Enterprise Security Organizations, The Alliance for EnterpriseSecurity Risk Management, http://www.asisonline.org/newsroom/alliance.pdf (verificado 12/03/08)

[6] ISA SP-99, (2005) Guide to the ISA-99 Standards Manufacturing and Control Systems Security, Instrumentation Society of America, www.isa.org/link/Guideto99 (verificado 12/03/08)

[7] Leiner, B. M. Cerf V. G. Clark D. D. Kahn R. Kleinrock L. Lynch D. C. Postel J. Roberts L. G. Wolff S, (2003), A Brief History of the Internet, Internet Society. http://www.isoc.org/internet/history/brief.shtml (verificado 12/03/08)

[8] Nascimento, A., Passito A., Mota, E., Nascimento, E., Carvalho L., (2006) Can I Add a Secure VoIP Call?, Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06),IEEE Computer Society http://delivery.acm.org/10.1145/1140000/1139435/25930435.pdf?key1=1139435&key2=4707229611&coll=GUIDE&dl=GUIDE&CFID=11885999&CFTOKEN=63519200 (verificado 12/03/08)

[9] Schultz, E, (2006), Convergent Security Risks in Physical Security Systems and IT Infrastructures, The Alliance for Enterprise Security Risk Management. http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=29115 (verificado 12/03/08)

[10] Schwartz, J, (2006),The Network is the Computer, Sun Microsystems, Inc, http://blogs.sun.com/jonathan/entry/the_network_is_the_computer (verificado 12/03/08)

[11] Teumin, D. J., (2005) Industrial Network Security, Instrumentation Society of America

[12] Williams, R. V.(2002), Chronology Of Information Science And Technology, School of Library and Information Sciences, University of South Carolina, http://www.libsci.sc.edu/bob/istchron/ISCNET/ISCHRON.HTM (verificado 12/03/08)

Enrique Daltabuit. *Egresado de la Facultad de Ciencias de la U.N.A.M. y doctorado en Física en la Universidad de Wisconsin en Madison; Director de Computo para la Investigación y luego de Telecomunicaciones en la U.N.A.M.; Coordinador del Diplomado en Seguridad de la Información del CEM Polanco de la U.N.A.M.; editor y coautor del libro "Seguridad de La información"; autor de varias publicaciones arbitradas sobre la seguridad de la información y sus implicaciones; profesor del Posgrado en Ciencias e Ingeniería de la Computación en la U.N.A.M.*