La convergencia en las aplicaciones electrónicas y la seguridad informática

Jorge Esteban Eterovic

A partir del cambio más importante que ha experimentado la sociedad en el ámbito de la información en esta última década, como lo es el surgimiento, desarrollo y globalización de Internet, nos estamos habituando a escuchar cada vez con mayor asiduidad términos que hacen referencia a aplicaciones electrónicas tales como: e-commerce, e-business, e-learning, e-banking, e-procurement, e-marketplace, e-government, e-vote, e-job, e-recruitment, entre otras, destinadas a ser el futuro motor de la economía mundial de los mercados abiertos.

Esta sinergia, desarrollada a partir del espacio que comparten las ciencias de las telecomunicaciones y de la informática, nos ofrece una amplia oferta de servicios y potencialidades nuevas aún por descubrir y desarrollar. No obstante, el ciberespacio no es un ámbito ideal. Por el contrario, el desarrollo explosivo de nuevas aplicaciones han agudizado los problemas de seguridad informática que ya existían, pero en menor proporción y bastante acotados.

La apertura de Internet trajo asociado el descubrimiento de nuevas vulnerabilidades y el desarrollo de peligrosas amenazas a la que todos estamos expuestos por tratarse de un entorno abierto. Es sabido que no existe una red totalmente segura y que un canal de información es, simplemente por definición, inseguro. Esto plantea un gran desafío en que la seguridad y la protección de la información juegan un papel fundamental para el desarrollo de las nuevas aplicaciones electrónicas.

Las herramientas que permitirán salvaguardar la información, trabajar en forma segura sobre las redes inseguras y proteger nuestra intimidad son provistas por una nueva área del conocimiento llamada: seguridad informática.

La seguridad informática

La seguridad informática es un concepto que surge como necesario a partir de los aspectos descriptos en el punto anterior. Básicamente se puede entender la seguridad informática desde dos puntos de vista: la seguridad lógica y la seguridad física.

La seguridad lógica permite el estudio, diseño e implementación de Sistemas de Encripción y Firma Digital, desarrollos de aplicaciones sobre Redes Segurizadas y Pro-

tocolos Criptográficos. Para ello se basa en los principios básicos de la Matemática Discreta, la Teoría de la Información y el estudio de la Complejidad de los Algoritmos.

La seguridad física se ocupa de la protección física de los datos en el sistema informático y comprende los Planes de Contingencia y Recuperación de Desastres, las Políticas de Seguridad, las Políticas de Backup y las Políticas de Acceso. Además se han desarrollado otras disciplinas relacionadas y afines a la seguridad informática, tales como: el Derecho Informático, la Auditoria Informática, el Peritaje Informático y el Análisis Forense.

Como se ve, el problema de la seguridad informática involucra no sólo conocimientos tecnológicos, por lo que se lo debe estudiar en forma global. Comenzaremos analizando el estado del arte para poder plantear finalmente una prospectiva.

El problema de la seguridad informática

Internet permite el acceso casi irrestricto a la información, su alcance llega tanto a las organizaciones, que se benefician con una presencia global y el acceso a nuevos mercados y clientes, como a la sociedad en su conjunto, que se beneficia de un acceso mayor y más rápido a todo tipo de información, productos y servicios.

Esta apertura global también significa un gran número de amenazas para los datos y la información confidencial de una organización, lo que obliga a disponer de un sistema de seguridad que los proteja de los distintos tipos de ataques.

Los riesgos a los que nos encontramos expuestos son muchos, y a manera de ejemplo se pueden describir los siguientes:

- Desde una PC ubicada fuera de una organización, se puede tomar el control de cualquier PC dentro de la misma.
- Se puede mandar un correo electrónico en nombre de otro y/o anónimo.
- En minutos, un hacker puede conocer las contraseñas de equipos y programas.
- Los mensajes de correo electrónico y los documentos transmitidos electrónicamente pueden ser "vistos y modificados" en cualquier punto de la red por donde viajen.
- Un usuario puede infectar con un virus informático la red de la organización.
- La mayor parte de los fraudes son a través del uso de los sistemas informáticos.
- Un hacker puede dejar los sistemas sin servicios.
- Una compañía puede ser demandada por incumplimiento de leyes y reglamentaciones (habeas data, propiedad intelectual).
- Se pueden robar o extraviar computadoras portátiles que contienen información crítica de la organización y claves de acceso a los sistemas protegidos.
- Se puede acceder indebidamente a la red de la organización desde Internet o a través de un módem conectado a la red telefónica.
- Todas las comunicaciones pueden ser interceptadas, incluso las satelitales.
- Los equipos informáticos pueden sufrir caídas o destrucciones.
- Los programadores pueden desarrollar programas tipo "bombas lógicas".
- Existen programas llamados "troyanos", que capturan información sensible.

- Se pueden hacer "escuchas" de comunicaciones de voz y de datos.
- Los comprobantes legalmente requeridos pueden no estar disponibles.
- La información impresa puede ser copiada.
- En los equipos puede haber instalado software sin licencias.
- La propiedad de la información y los desarrollos a favor de las organizaciones pueden no estar asegurados.
- El personal contratado puede no tener suficientes niveles de seguridad en sus equipos y en las aplicaciones que acceden.
- Los empleados y terceros contratados pueden no haber firmado contratos de confidencialidad.
- Los soportes de la información pueden ser robados o destruidos.
- Se puede distribuir información alterada a socios, accionistas, auditores y entes de control.
- Se puede no disponer de la información en el momento adecuado.
- Puede haber envíos de e-mails desde la organización con información sensible o con agresiones a terceros.
- Se pueden distribuir datos con información privada de los empleados.
- Se puede obtener la documentación impresa de la basura.
- Alguien puede acceder a la información no recogida de las impresoras.

Considerando que el aumento de la oferta de productos y servicios a través de Internet ha cambiado la forma de relacionarse entre las empresas, sus clientes y sus proveedores y ha convertido a la red en un canal que se usa cada vez más para las aplicaciones tradicionales, es muy importante tener presente las vulnerabilidades de los sistemas y los riesgos a los que nos exponemos.

Actualmente se está produciendo un crecimiento sostenido de las transacciones electrónicas, que se inicia con el acceso a Internet del público en general y es algo que está revolucionando el ámbito del comercio global y de la economía. Como todo parece indicar que las aplicaciones electrónicas serán uno de los mercados de desarrollo más importantes en el mediano plazo, uno de los aspectos que más debe preocupar es la seguridad de las transacciones electrónicas. ¿Como evitar los temibles hackers?, ¿los robos de datos? o ¿cuál es la mejor manera de configurar un servidor web en forma segura?

Estas cuestiones no están del todo resueltas para los responsables de los sistemas informáticos y menos aún para los usuarios comunes, que aún siguen sumidos en el desconocimiento. Por ello, ante la aparición de una nueva amenaza, inmediatamente se produce un descenso de la proyección de negocios de cualquier empresa.

Si tomamos como ejemplo el e-commerce, en la actualidad, la forma de pago más frecuente entre los compradores virtuales es la tarjeta de crédito, que se utiliza en un 46% de los casos, seguida del contrarreembolso en un 35%, y tan sólo en un 13% la transferencia bancaria. La plena implantación de los medios de pago cuenta con varios frenos, entre los que se destaca la seguridad en este tipo de transacciones, un problema que preocupa tanto a las entidades financieras, por el alto porcentaje de denegación de pago que reciben, como a los consumidores, que temen comunicar sus datos bancarios por Internet. Por

ello, los expertos en materia de seguridad establecen cuatro requisitos fundamentales para conseguir que una transacción comercial por Internet pueda considerarse segura:

1. identificar al comprador y al vendedor,
2. asegurar la integridad de la información que se intercambia,
3. asegurar su confidencialidad y
4. garantizar el no rechazo.

Actualmente el comercio electrónico superó la etapa inicial, pero aún no está afianzado suficientemente como una parte importante de los procesos de negocio de las empresas. Faltan regulaciones y protecciones legales en muchas áreas, especialmente en las transacciones de los consumidores en Internet. Existe una limitada experiencia de cómo definir contratos en el entorno electrónico; las empresas no saben qué políticas implementar y hay una carencia de historia a largo plazo sobre las relaciones y contactos que no son cara a cara. No es exagerado decir que la confiabilidad, más que la tecnología, marca el ritmo del crecimiento del comercio electrónico en todas sus formas.

Los negocios en la red están creciendo día a día y todos quieren estar ahí, pero antes de dar ese paso, es necesario comprender cuáles son las tecnologías, los estándares y las regulaciones con las que se manejan los negocios en línea, para brindar la seguridad necesaria a todos los participantes.

Uno de los aspectos que debemos analizar es el marco jurídico y normativo que regulan los principales elementos implicados en los intercambios seguros de información en Internet, y más concretamente en los escenarios propios de las aplicaciones electrónicas, como el comercio electrónico.

El marco legal de la seguridad informática

Actualmente el marco legal que permite el desarrollo de las aplicaciones electrónicas está conformado por las siguientes leyes y normas:

Ley/Norma	Descripción	Estado actual
Ley 11.723	Régimen Legal de la Propiedad Intelectual	Promulgada el 28 de setiembre de 1989
Ley 25.036	Ley de Propiedad Intelectual, modificatoria de la Ley 11.723	Promulgada en noviembre de 1998
Ley 24.766	Ley de Confidencialidad sobre Información y Productos	Promulgada el 20 de diciembre de 1996
Decreto 427	Infraestructura de Firma Digital para el Sector Público Nacional	Vigente desde 16 de abril de 1998
Ley 25.326	Ley de Protección de los Datos Personales (Habeas Data)	Vigente desde 30 de octubre de 2000
Ley 25.506	Ley de Firma Digital	Promulgada el 11 de diciembre de 2001. Reglamentada en diciembre de 2002
Ley 25.856	Ley de la producción de software como actividad industrial	Promulgada el 6 de enero de 2004
	Ley de Delitos Informáticos Diputados	Con media sanción en
	Ley de Protección del Correo Electrónico	Con media sanción en Diputados
Resolución AFIP 1361	Norma que autoriza a almacenar el duplicado de las facturas en formato digital	Rige a partir del 1 de abril de 2003
ITU-T X.509	Data Networks and Open System Communications	Estándar de uso mundial
IRAM 17799	Norma ISO-IRAM de Seguridad Informática	Estándar mundial homologado por IRAM

Del análisis del cuadro precedente surge claramente que existe un vacío legal importante debido a que dos leyes fundamentales, tales como la de Protección del Correo Electrónico y la de Delitos Informáticos, están a la espera de su sanción definitiva.

También se debe considerar como muy importante que se creen y mantengan operativos los organismos de fiscalización y control que prevén estas leyes, para garantizar su cumplimiento efectivo.

El estado del arte de la seguridad informática

A nivel mundial, a partir de los atentados terroristas del 11-S ocurridos en los Estados Unidos, la demanda de soluciones de seguridad informática creció casi un 40%. Los analistas afirman que fue uno de los segmentos mas rentables del sector tecnológico en un año con depresión. Según la consultora IDC, las compañías que desarrollan soluciones de seguridad tanto de software como de hardware, vieron crecer notablemente su negocio.

Las áreas de software de mayor crecimiento fueron los sistemas de back-up, las soluciones para la recuperación de datos en caso de desastres y las aplicaciones para evitar las intrusiones a los sistemas informáticos. Dentro del hardware de autenticación, la biometría ha sido el sector más beneficiado.

Según un estudio de la consultora Gartner Dataquest, el 14% de las empresas en el mundo invirtieron para mejorar sus planes de seguridad. De éstas, el 41% invirtió en nuevos equipos de seguridad, el 18% contrató servicios de consultoría para analizar planes de seguridad y de recuperación de datos en caso de desastres y el 9% contrató personal especializado en temas de seguridad.

En nuestro país no existen datos estadísticos en ésta área. Pero de manera indicativa sirven los valores obtenidos por la consultora Ernst & Young sobre 273 empresas de distintos sectores y países, entre los que se incluía la República Argentina. Según el estudio, el 40% de las empresas consideraba como un problema grave la seguridad informática, pero el "gasto" en seguridad informática sólo es de entre el 4 y el 10% del gasto total en informática.

Del total de empresas encuestadas, el 72% se mostró reacia a admitir que sus sistemas habían sido saboteados y el 79% cree que existen mayores posibilidades de sufrir un ataque informático desde el exterior de la empresa, lo que representa un grave error. El 80% de las empresas manifestó no haber experimentado un ataque de intrusión a sus sistemas informáticos, pero paradójicamente solo el 33% admitió estar en capacidad de detectar dicho tipo de ataque.

Finalmente, sólo el 39% de las empresas consultadas usa algún software estándar de seguridad y nada mas que el 20% de ese total hace un uso avanzado de estas herramientas.

Tecnologías usadas en seguridad informática

A efectos de analizar la forma en que las organizaciones están usando las distintas tecnologías disponibles en el área de la seguridad informática, nos basamos en el informe anual del CSI/FBI (Computer Security Institute / Federal Bureau of Investigation) denominado Computer Crime and Security Survey.

Según dicho informe, actualmente se están usando las siguientes tecnologías:

- Control de accesos
- Biometría
- Encriptación de archivos
- Software antivirus
- Passwords reusables
- Firewalls
- Login encriptado
- Seguridad física
- PCMCIA
- IDS-sistemas de detección de intrusos
- ID digitales

A partir del punto siguiente se describirán someramente cada una de ellas.

Del análisis de dicho informe se concluye que casi la totalidad de las organizaciones usan software antivirus y tienen al menos un Firewall instalado. Es importante destacar

que el 91% emplea alguna clase de seguridad física para proteger sus computadoras y sus activos informáticos y el 92 % emplea alguna medida de control de acceso.

Es notable cómo algunas tecnologías ha sido rápidamente adoptadas, tal es el caso de los sistemas de detección de intrusos (IDS), que se encuentran en el 73% de las organizaciones. Sin embargo otras tecnologías, como los identificadores biométricos, solo han sido implementados en un escaso 11%.

Se trata generalmente de empresas que hacen uso intensivo de las formas más avanzadas de seguridad informática, ya que de este grupo el 72% utiliza ID digitales o certificados digitales y el 83% aplica encriptación a sus archivos de datos. Sin embargo si analizamos estas dos últimas tecnologías en el conjunto de todas las organizaciones relevadas, observamos que sólo alcanza el 49% el ID digital y el 69% la encriptación de archivos.

El gráfico del Anexo 1 muestra en perspectiva la evolución de las distintas tecnologías usadas en seguridad informática en los últimos cinco años.

Tecnología de control de acceso

Esta tecnología se refiere a las Listas de Control de Accesos, que proveen un nivel de seguridad adicional a los niveles de seguridad clásicos provistos por los Sistemas Operativos.

Estas listas permiten definir permisos a usuarios y grupos concretos; por ejemplo, pueden definirse sobre un servidor Proxy una lista de todos los usuarios (o grupo de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características, como limitaciones de anchos de banda y de horarios.

Tecnología de biometría

Originariamente esta tecnología hacía referencia a la aplicación de las matemáticas y las estadísticas en el análisis de datos de las ciencias biológicas. Actualmente se refiere a la aplicación de técnicas para la verificación y autenticación automática de la identidad de las personas.

Los sistemas biométricos se basan en medir, directa o indirectamente, ciertas características morfológicas y/o determinadas pautas de comportamiento del usuario, aplicando la estadística, la inteligencia artificial y el reconocimiento de patrones. Analizan y miden ciertos rasgos unívocos de un individuo para crear un identificador biométrico irrefutable, una especie de patrón numérico. Este identificador puede luego almacenarse en una base de datos y recuperarse para su posterior comprobación.

Las tecnologías biométricas se pueden agrupar en dos categorías, estáticas y dinámicas. La biometría estática mide la morfología del usuario, y entre ellas se encuentran: huella digital, geometría del dedo, geometría de la mano, termografía de la mano, venas del dorso de la mano, análisis del iris, análisis de la retina, reconocimiento facial, termografía de la cara, geometría de la oreja y geometría del cuerpo.

La biometría dinámica mide el comportamiento del usuario, y tenemos: patrón de voz, firma manuscrita, dinámica de tecleo, movimiento de los labios, análisis gestual y forma de caminar.

Tecnología de encriptación de archivos

También conocida como criptografía, es una ciencia que trata sobre la protección de la información transformando un archivo o mensaje inteligible en otro que no lo es, mediante el uso de algoritmos y claves. Entre las disciplinas involucradas están: la teoría de la información, la matemática discreta, la teoría de los números primos muy grandes y la complejidad computacional.

Existen dos tipos básicos de sistemas criptográficos. Los simétricos o de clave privada (secreta), que usan la misma clave para cifrar y descifrar. Los sistemas asimétricos o de clave pública y privada emplean una doble clave, una de ellas para el cifrado y la otra para el descifrado, siendo en muchos sistemas intercambiables, es decir que si se usa una para cifrar, con la otra se puede descifrar y viceversa.

En los algoritmos que usan claves asimétricas, éstas son de un tamaño diez veces mayor a las usadas por los sistemas simétricos. Esto sumado al hecho que normalmente se hace una doble encriptación, se traduce en que los sistemas simétricos son mucho mas rápidos, pero tienen una muy mala gestión de intercambio de claves. En la práctica se emplea una combinación de ambos sistemas.

Tecnología de software antivirus

Los virus informáticos son pequeños programas, invisibles para el usuario, que actúan de forma subrepticia y cuyo código incluye información que les permite autorreproducirse y mutar. Son capaces de modificar, alterar y/o borrar programas e información, además de afectar el normal funcionamiento del hardware. Normalmente tienen tres módulos: de reproducción, de ataque y de defensa.

Las técnicas de propagación de los virus son varias, y cada vez son más ingeniosas y dañinas. Tradicionalmente usaban para su diseminación los disquetes y los medios removibles, pero actualmente hacen uso intensivo del correo electrónico, el chat, los grupos de noticias y las páginas web.

Los software antivirus se basan en una gran base de datos con la firma (cadena de caracteres propios de cada virus) de todos los virus conocidos para identificarlos y poder así neutralizarlos o eliminarlos. Esta técnica es reactiva, por lo que siempre los virus van un paso adelante. Actualmente se han desarrollado nuevas técnicas conocidas como heurísticas, que brindan una forma de adelantarse a los nuevos virus a partir del análisis y detección de ciertas actividades sospechosas, características del accionar de los virus informáticos.

Las principales funciones de un programa antivirus son: la detección, la identificación mediante el scanning del código de todos los archivos o de la heurística y el chequeo de la integridad del sistema.

Tecnología de passwords reutilizables

Las passwords reutilizables son la principal herramienta de control de acceso de la mayoría de los sistemas desde hace muchos años, a pesar de los avances tecnológicos producidos en todas las áreas. En los tiempos de los mainframe y de las terminales "bobas" eran lo suficientemente eficientes, pero con el advenimiento de los sistemas cliente/servidor, ya las passwords reutilizables no tienen mucho sentido, porque las mismas viajan por la red LAN y por Internet como texto claro, siendo fácilmente capturadas por programas robot de fácil obtención.

Las debilidades de las passwords reutilizables son muchas. Las estadísticas demuestran que muchos usuarios tienden a escoger contraseñas muy débiles, las comparten con sus compañeros y hasta las dejan anotadas en lugares de fácil acceso.

Una forma de dar más seguridad a las passwords reutilizables es desarrollar e implementar políticas específicas tales como longitud mínima, combinación de números y letras, uso de mayúsculas y minúsculas, vencimiento, llevar un histórico de contraseñas para evitar su repetición y concienciar a los usuarios sobre las implicancias de compartir contraseñas y de usar contraseñas débiles.

Tecnología de Firewall

Es uno de los elementos más importantes de la seguridad informática, pero se les debe prestar mucha atención, porque no son la solución definitiva a los problemas de seguridad, ya que nada pueden hacer contra los ataques desde adentro de red LAN o contra las técnicas de ingeniería social. Sólo sirve como defensa perimetral de las redes.

Un Firewall es un elemento de hardware, de software o una combinación de ambos, que tiene como misión básica separar dos redes, una insegura como lo es Internet y otra que queremos asegurar, nuestra LAN y que funciona de acuerdo con las políticas de seguridad establecidas.

Funciona mediante reglas que se pueden ir actualizando. Básicamente funcionan según uno de los dos siguientes principios: todo lo que no está específicamente prohibido, está permitido, o todo lo que no está específicamente permitido está prohibido.

Pueden tener capacidades adicionales, como la encriptación del tráfico de la red, para lo cual si dos Firewalls están conectados, ambos deben usar el mismo método de encriptación-desencriptación para poder entablar la comunicación.

Existen dos tipos de Firewalls. Los que hacen filtrado de paquetes basándose en los protocolos utilizados, las direcciones IP de origen y destino o los puertos TCP o UDP de origen y destino. El otro tipo de Firewall se encarga de filtrar las conexiones y se lo

denomina Proxy. Su función es analizar el tráfico de red en busca de contenidos que violen la seguridad de la misma, actuando de intermediario entre el cliente y el servidor real de la aplicación, siendo su funcionamiento transparente para ambas partes.

Tecnología de login encriptado

Es una de las herramientas más importantes para los accesos remotos seguros a los servidores internos de las empresas, ya sea por líneas dedicadas o a través de Redes Privadas Virtuales (VPN). Los protocolos de login encriptado tales como Kerberos, SSH / TTL o IPSec, son utilizados para controlar los accesos vía Telnet, SNMP y HTTP.

Los beneficios en infraestructura y costos que ofrece la implantación de Redes Privadas Virtuales como soporte de las comunicaciones corporativas necesitan de una fuerte garantía de seguridad para que haga factible su empleo, cuando el medio sobre el que se montan es totalmente abierto e inseguro. El factor crítico en la operación de las VPN no está en el túnel de conexión, sino en los mecanismos de seguridad tales como login encriptados, que preservan la confidencialidad e integridad de la comunicación.

Tecnología de seguridad física

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos y a la información confidencial.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza. Dentro del grupo de amenazas humanas tenemos el robo, el fraude, el sabotaje, que pueden ser de origen interno o externo a la organización; también se debe considerar como una amenaza la impericia y/o falta de conocimientos suficientes de los empleados. Para contrarrestar estas amenazas se deben adoptar una serie de procedimientos de prevención y control físicos y lógicos.

Entre las amenazas naturales se consideran: incendio, inundaciones, condiciones climatológicas extremas, terremotos, cortes de energía eléctrica, señales de radar, entre los más importantes. La mejor forma de hacer frente a este tipo de amenazas consiste en hacer un buen diseño y planeamiento de la ubicación e instalación del centro de cómputos, tener elaborado y probado un plan de contingencias y de recuperación ante desastres y contar con todos los procedimientos actualizados y periódicamente chequeados.

Tecnología de PCMCIA

Este elemento de seguridad informática consiste en una tarjeta inteligente PCMCIA con un sistema de encriptación de clave pública. Es utilizada como un método seguro de

autenticación tanto para estaciones de trabajo fijas como móviles, cuando necesitan acceder a aplicaciones y programas a través de redes inseguras, como Internet.

Son muy flexibles ante las actualizaciones de la infraestructura de seguridad informática y permiten dar un alto grado de protección a un amplio rango de aplicaciones, tales como administración de passwords, autenticación de hosts, log-on a sistemas, accesos VPN, autorización web, seguridad del equipo, integración con sistemas biométricos, encriptación con sistemas de clave pública y privada de hasta 2048 bits, certificados digitales y firma digital.

Tecnología de IDS

Es otro de los elementos importantes de la seguridad informática. Consiste en sistemas capaces de detectar actividades inapropiadas, incorrectas o anómalas, ya sea desde el exterior como desde el interior del sistema informático.

Estos sistemas de detección de intrusos según su función pueden estar basados en máquinas, para detectar actividades maliciosas en las aplicaciones de las mismas, o bien basados en la red, para analizar el flujo de información intercambiada en la misma.

Según su comportamiento, estos sistemas pueden estar basados en conocimiento o en comportamiento, tratando de detectar actividades intrusivas pero no anómalas, actividades no intrusivas y anómalas y actividades intrusivas y anómalas. Es mucho más costoso desde el punto de vista del gasto computacional la detección de actividades anómalas, ya que se deben seguir distintas métricas par determinar cuánto se aleja el usuario de lo que se considera su comportamiento normal.

Tecnología de ID digitales

Un digital ID, también llamado certificado digital, es un adjunto a un mail o programa en una página web que verifica que el destinatario o sitio web es quien realmente dice ser. Consiste en un código secreto que se interpreta por el software criptográfico del navegador web o programa de correo.

Un digital ID no garantiza la calidad del software o de la información, pero verifica la identidad del propietario del certificado. En el caso de transacciones con tarjeta de crédito, la modalidad de digital ID es utilizado SSL Server Certificate. En un correo personal certificado, el digital ID es usado para encriptar el correo saliente.

Cuando un cliente desea realizar una compra mediante tarjeta de crédito, enviando información confidencial, querrá garantizarse una conexión segura. La tecnología SSL es utilizada para proteger este tipo de información confidencial.

La encriptación SSL utiliza un sistema único de claves (públicas y privadas) para verificar las comunicaciones entre el servidor y el cliente. Estas claves se usan sólo una vez durante una sesión con el cliente. Haciendo esto, la información no puede ser vista por terceros. Bajo una conexión SSL ambas partes saben que solamente ellos están vien-

do lo que el otro ha enviado. Si ocurriese alguna alteración en la encriptación, se generaría automáticamente un mensaje de error.

La situación en la Argentina

Encuestas recientes del CISIAR, organización dedicada a la investigación en seguridad informática, revelan que el 47% de las empresas manifestó haber tenido incidentes de seguridad informática en el último año. De éstas el 52% citó como primera fuente de ataque a Internet.

Los ataques más comunes durante el último año fueron los virus informáticos y el *spamming* en el correo electrónico.

Las tecnologías de seguridad más utilizadas actualmente son: Password reusable, Software Antivirus y Firewalls. Actualmente, los problemas experimentados por motivos de seguridad van desde ataques externos, hasta incidentes desde el interior de la propia organización, como aquellos provocados por las empleados que borran archivos críticos o acceden a información confidencial.

En ese contexto, la seguridad informática resulta vital, en tanto los riesgos y vulnerabilidades pueden significar millonarias pérdidas y comprometer la continuidad del negocio.

Conclusiones

El problema de la seguridad informática lo debemos analizar desde distintos puntos de vistas, que son el legal, el económico y el tecnológico.

Ya algo se ha dicho del marco jurídico. Es fundamental que las leyes se aprueben y entren en vigencia para regular las operaciones que hacen uso de las aplicaciones electrónicas. Esto debe ser un esfuerzo conjunto entre los legisladores y los técnicos, que deberán comprometerse desde las distintas cámaras empresarias y asociaciones profesionales para asesorar adecuadamente en cada uno de los temas planteados. Como ejemplo, existe un anteproyecto de la futura Ley de Protección del Correo Electrónico, que en su afán por garantizar la privacidad de las personas impide que se realice un control de seguridad del e-mail corporativo para evitar la fuga de información sensible de las organizaciones.

Para destacar, ya se ha creado la Dirección Nacional de Protección de Datos Personales, para proteger el derecho a la privacidad de las personas y también el derecho al acceso a las bases de datos y la Ley de Firma Digital crea el marco adecuado para el desarrollo del comercio electrónico.

Desde el punto de vista económico, cuanto mayor sea el crecimiento de las aplicaciones electrónicas, más importante se volverá todo lo relacionado con la seguridad informática, ya que el incremento de los riesgos tecnológicos significa un aumento de los riesgos comerciales.

Las aplicaciones electrónicas son completamente dependientes de las relaciones establecidas entre las partes involucradas y cambia muchas de las reglas básicas de las formas de operar en general y de los negocios en particular, lo que significa que deberán cambiar muchas de las reglas de seguridad, contabilidad y control financiero. Un ejemplo de ello es la norma conocida como Sabarney-Oxley Act, para el control antifraude financiero.

Finalmente el aspecto tecnológico se debe abordar desde dos perspectivas. En todo lo relativo a la seguridad lógica, han comenzado a trabajar algunas PyMES con personal altamente capacitado, desarrollando e implementando soluciones de seguridad locales, que seguramente se beneficiarán con la Ley de Desarrollo de la Industria del Software, ya que contarán con mejores condiciones para exportar sus productos y servicios.

En el campo de la seguridad física, la mayoría de los sistemas son de origen extranjero, pero con el cambio de las condiciones económicas en nuestro país también se han comenzado a desarrollar productos locales y aumentar considerablemente el mantenimiento de los sistemas instalados, la capacitación y los servicios de consultoría.

Como no se pueden predecir todas las amenazas, lo aconsejable es planificar sobre la base de las tendencias, y elaborar las prospectivas para que las soluciones de seguridad informática puedan hacer cada día más seguras las aplicaciones electrónicas.

Bibliografía

Cryptography and Network Security - Principles and Practice. 3ª edition. Stallings, William. Editorial Prentice-Hall Inc., Nueva York, 2002.

IRAM-ISO/IEC 17799 – "Tecnología de la información norma argentina". IRAM, Buenos Aires, 2002.

Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados. 1ª edición. Siles Peláez, Raúl. GNU Free Documentation License. 2002.

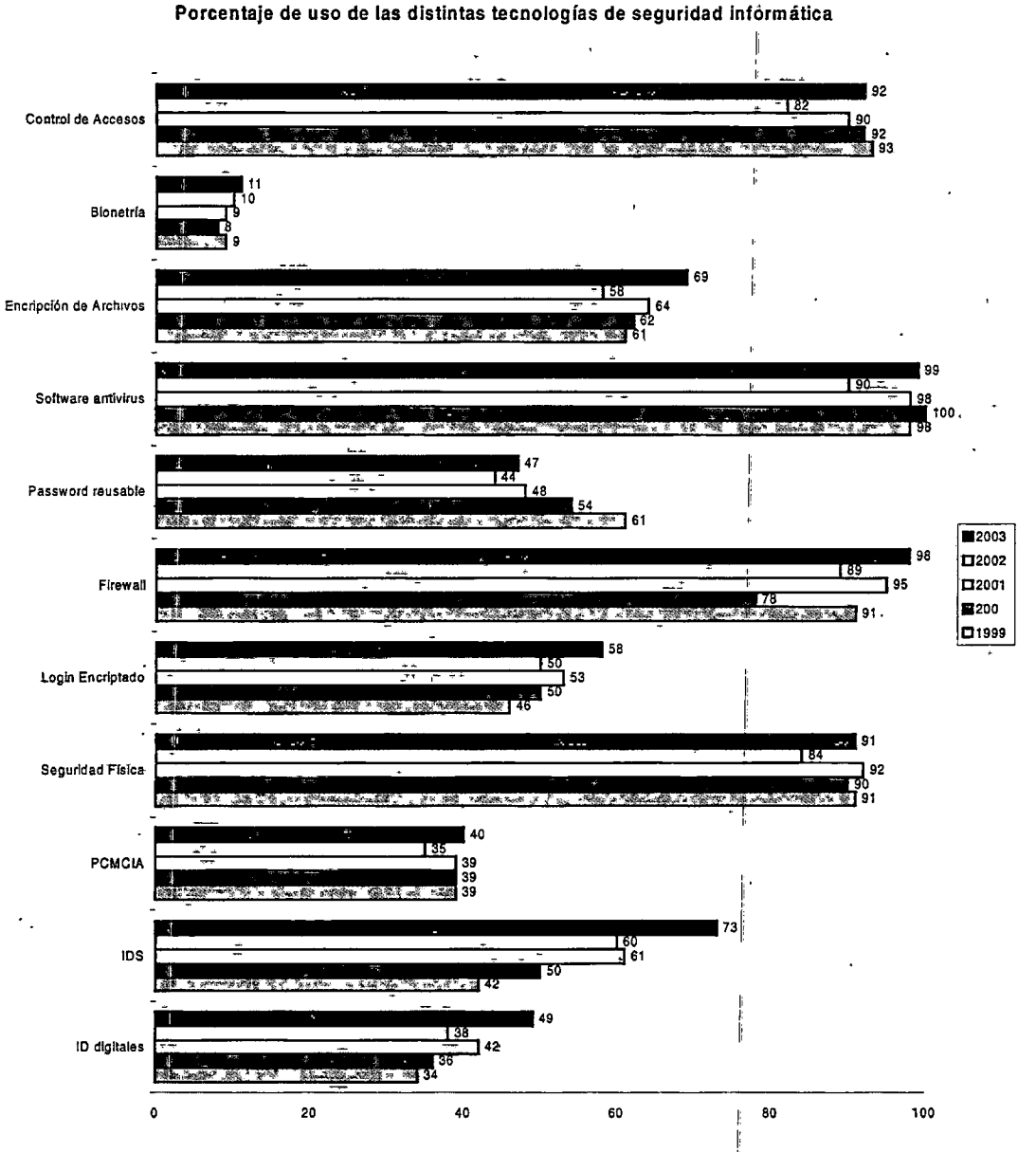
Hackers 4 - *Secretos y soluciones para la seguridad de redes*. McClure, Stuart; Kurtz, George; Scambray, Joel. Editorial Mcgraw-Hill. 2003.

Diseño de seguridad en redes. Kaeo, Merike. Editorial Pearson Educación. 2003.

2004 CSI / FBI. *Computer Crime and Security Survey*. Computer Security Institute. 2004.

"Computer security incident handling. Recommendations of the National Institute of Standards and Technology". Grance, Tim; Kent, Karen; Kim, Brian. NIST. Gaithersburg, MD. 2004.

Anexo 1


Porcentaje de uso de las distintas tecnologías de seguridad informática
Control de Accesos
92
82
90
92
93
Biometría
11
10
9
8
9
Encripción de Archivos
69
58
64
62
61
Software antivirus
99
90
98
100
98
Password reusable
47
44
48
54
61
Firewall
98
89
95
78
91
Login Encriptado
58
50
53
50
46
Seguridad Física
91
84
92
90
91
PCMCIA
40
35
39
39
39
IDS
73
60
61
50
42
ID digitales
49
38
42
36
34
0
20
40
60
80
100
2003
2002
2001
200
1999