CONFIANZA EN EL CIBERESPACIO

Fuente: http://www.bsa.org/seguridad/

Introducción

.....

Nunca antes la seguridad de las redes y de la computación tuvo una importancia tan primordial.

Las innumerables operaciones diarias, desde el funcionamiento de los mercados financieros hasta el suministro constante de agua y electricidad a nuestros hogares, requieren sistemas informáticos seguros y confiables. Las compañías que integran BSA construyen muchas de esas redes que alimentan las infraestructuras de información en el mundo, incluyendo Internet, y desarrollan las principales herramientas de seguridad utilizadas para proteger las redes informáticas contra delitos y ataques cibernéticos.

Obtenga más información sobre lo que hacen BSA y sus miembros para promover la seguridad en el ciberespacio y sobre lo que pueden hacer las autoridades responsables para garantizar un mundo en línea lícito y seguro.

Cómo construir un mundo en línea lícito y seguro

Garantizar la seguridad y la protección de datos de las redes y la computación es una de las prioridades más importantes de BSA y sus compañías asociadas.

La importancia de salvaguardar la computación y las redes globales no debe ser subestimada, especialmente a raíz de la experiencia de los trágicos acontecimientos mundiales desencadenados en septiembre del 2001. Innumerables operaciones diarias, desde el libre funcionamiento de los mercados financieros hasta el suministro constante de agua y electricidad a nuestros hogares, requieren redes de información seguras.

Como desarrolladores de muchos de los productos, redes y sistemas que alimentan las infraestructuras de información del mundo, y de las principales herramientas de seguridad utilizadas para protegerlos, los asociados de BSA tienen un compromiso único con la seguridad en el ciberespacio. De hecho, los Directores Generales de las compañías asociadas con BSA han desarrollado un programa de seguridad en el ciberespacio que consta de recomendaciones específicas sobre políticas que apuntan a hacer que América sea más segura (haga clic aquí para ver el programa). Además, BSA ha desarrollado "listas de verificación" de seguridad en el ciberespacio que pueden utilizar consumidores, empresas grandes, medianas y pequeñas y gobiernos para mejorar su propia seguridad en el ciberespacio (haga clic aquí para ver las listas de verificación).

El éxito de Internet depende de su seguridad

Quizás en ningún lugar sea más frecuente la amenaza del uso indebido de la computación y los delitos informáticos que en Internet. Y sin embargo, el éxito de Internet dependerá de muchas maneras de la confianza depositada en ella por las personas, las empresas y los gobiernos. Para que exista esa confianza, la información de

usuario transmitida por las redes informáticas deberá estar a salvo de ladrones, hackers y otras personas que pudieran obtener acceso y hacer uso de información confidencial sin permiso. Los consumidores necesitan confiar en que la información personal suministrada para las transacciones permanecerá segura, al igual que las empresas necesitan confiar en que sus conexiones con los proveedores y los clientes no serán interrumpidas.

Las violaciones de la protección de datos y la seguridad en el ciberespacio, ya sea a través de Internet o de otras redes informáticas, se pueden producir de diversas maneras, incluyendo acciones de hackers, ataques de denegación de servicio, virus y gusanos.

- Las **"acciones de hackers"** sobre los sistemas informáticos y los sitios web son prácticas cada vez más comunes en las que personas o pequeños grupos tratan de obtener acceso no autorizado, a menudo con fines de vandalismo o robo de información.
- Los **ataques de denegación de servicio** son esfuerzos concertados a gran escala para paralizar un sitio web, normalmente un sitio comercial de renombre, sobrecargándolo con información proveniente de muchas fuentes.
- Los **virus y gusanos** son pequeños programas de computadora que se duplican automáticamente, generalmente concebidos para propagarse por correo electrónico y provocar daños en los sistemas informáticos de usuarios desprevenidos.

  Haga clic aquí para obtener más información sobre las principales amenazas a la seguridad.

¿Cómo pueden las personas, las empresas y los gobiernos ayudar a proteger sus computadoras y redes?

El proceso de garantizar la seguridad en el ciberespacio es continuo, no es una reparación que se haga una sola vez. La seguridad en el ciberespacio exige la adopción de firmes políticas de seguridad, la implementación de mecanismos y software de seguridad en el ciberespacio de comprobada eficacia (tales como antivirus, firewalls, detección de intrusión, encriptación, infraestructura de clave pública (PKI) y administración de la vulnerabilidad), y, en el caso de organizaciones más importantes, la existencia de profesionales de seguridad capacitados. Y estos profesionales deberán recibir capacitación constante para garantizar que puedan detectar y combatir la naturaleza evolutiva de las amenazas en el ciberespacio.

Pero mientras que garantizar la seguridad en el ciberespacio es un proceso continuo, no es uno complejo. De hecho, la clave para mejorar la seguridad de las redes informáticas reside en tres principios fundamentales:

- Los gobiernos pueden ayudar a los usuarios a protegerse y deben predicar con el ejemplo;
- La tecnología faculta a las personas a protegerse por sí mismas; y
- La industria, a través del mercado, puede ir al frente de todos.

Principales amenazas para la seguridad en línea

Los ataques en el ciberespacio se clasifican en varias categorías: (1) **acciones accidentales** y (2) **ataques maliciosos**. En esta última categoría existen numerosos subgrupos, incluyendo virus informáticos, ataques de denegación de servicio y ataques de denegación de servicio distribuida. Una tercera área de vulnerabilidad en el ciberespacio, el **fraude en línea**, comprende asuntos como robo de identidad y robo de datos.

I. Acciones accidentales

Las acciones accidentales contribuyen a una gran cantidad de riesgos de seguridad informática. Esta categoría abarca problemas que surgen de la falta de conocimiento básico de los conceptos de seguridad en línea e incluye asuntos como malas elecciones de contraseña, transacciones comerciales accidentales o erróneas, divulgación accidental y software erróneo o desactualizado. Los problemas afines se producen como consecuencia de productos de seguridad mal configurados y fuga de información, debido a transferencias inseguras de información. La educación y la prudencia deben ser consideradas las defensas fundamentales para limitar la frecuencia y el alcance de dichos acontecimientos, ya que esta forma de vulnerabilidad del ciberespacio es en gran parte autoinflingida y evitable.

II. Ataques maliciosos

Los ataques cuyo objetivo específico es hacer daño se denominan ataques premeditados o maliciosos. También se pueden desglosar en ataques provocados por código malicioso y aquellos causados por información falsa intencional. La información falsa generalmente se observa con respecto al fraude en línea y el robo de identidad (ver más abajo). Por otra parte, el código malicioso es el origen de los llamados "crackings" y "hackings", cuyos ejemplos notables incluyen virus informáticos, robo de datos y ataques de denegación de servicio (DOS).

Virus informáticos

La forma más común de código malicioso es el **virus informático**, un programa o fragmento de código que se replica adjuntando copias de sí mismo a otros programas.

Existen cuatro clases principales de virus:

1. La primera clase denomina a los ***virus de infección de archivos***, que se incrustan en archivos ejecutables comunes y se adjuntan a los archivos ejecutables de otro sistema cuando se ejecuta el archivo.
2. La segunda categoría define a los ***virus de infección del sistema o el sector de arranque***, que infectan el primer sector de una unidad desde la que se arranca el sistema operativo. En la actualidad, estos virus no son tan comunes, debido a que los disquetes se utilizan con menor frecuencia.
3. El tercer grupo se refuere a los ***virus de macros***, los cuales infectan los archivos de datos que contienen "macros" para la creación de conjuntos de instrucciones.
4. Por último, los virus que utilizan más de un método de ataque se llaman ***virus multipartitos***.

El virus/gusano "Melissa", que en 1999 ocasionó aproximadamente $80 millones en pérdidas a nivel mundial, era un código malicioso incrustado en un documento de Word® que, al ser abierto, se enviaba como un archivo adjunto a las primeras cincuenta personas que figuraban en el libro de direcciones de un cliente de correo electrónico. El virus "I LOVE YOU", surgido en mayo del 2000, era aún más simple: un pequeño pedazo de código adjunto a un mensaje de correo electrónico. Al hacer doble clic en el archivo ejecutable enviaba un mensaje de correo electrónico a todas las personas que figuraban en un libro de direcciones, dañando posteriormente las máquinas de las víctimas. Los virus de rápida propagación como el "I LOVE YOU" hacen que los servidores de correo electrónico se sobrecarguen y las empresas deban interrumpir la recepción de correspondencia por correo electrónico. Por ejemplo, en un día, el virus "I LOVE YOU" ocasionó más de $100 millones en pérdidas tan sólo en en Estados Unidos y más de $1.000 millones a nivel mundial.

Ataques de denegación de servicio

Los **ataques de denegación de servicio**, otra forma de código malicioso, se construyen y ejecutan con esmero; estos ataques no son nuevos, sin embargo, son cada vez más sofisticados. Los ataques DOS tradicionales normalmente involucran una computadora que ataca a otra, pero cada vez es más común utilizar varias computadoras en un ataque que requiere gran organización. Dichos ataques, conocidos como **ataques de denegación de servicio distribuida (DDOS)**, fueron observados en varias paralizaciones de sistemas informáticos de grandes corporaciones en el año 2000.

Es importante comprender los componentes técnicos de un ataque de DDOS, ya que estos ataques revelan con precisión las vulnerabilidades inherentes a Internet. Un ataque de DDOS funciona sobrecargando un servidor con una avalancha de mensajes que parecen ser normales. El atacante de DDOS forma estratégicamente un ejército de jugadores clave que son:

1. una computadora *cliente* para coordinar el ataque;
2. de tres a cuatro computadoras *anfitrionas*, que son los campos de batalla bajo control directo del atacante; y
3. cientos de *difusores* potenciales, que son las legiones que ejecutan el código para generar el flujo excesivo de paquetes que atacan un sistema objetivo (que consta de una máquina como mínimo). Los difusores son reclutados por un software de exploración de puertos que determina las máquinas en las cuales el atacante puede obtener privilegios de raíz. En estas máquinas, el atacante puede incrustar programas ocultos que esperan instrucciones de las máquinas anfitrionas.

El atacante envía una lista de las direcciones de Protocolo de Internet (IP) de las máquinas objetivo a través de una fuerte encriptación. Con todos los componentes listos, el atacante instruye a cada máquina para que envíe, en forma simultánea, paquetes de datos contra las direcciones IP dadas utilizando direcciones de origen falsas, en un proceso conocido como "spoofing" (engaño). Como el ataque contiene demasiada información para procesar y se origina desde demasiadas máquinas distintas con direcciones IP fraudulentas, los servidores objetivo podrán sobrevivir el ataque únicamente si se desconectan de Internet o deniegan el servicio indiscriminadamente a todos los clientes que envían datos de entrada. Por lo tanto, el ataque de denegación de servicio distribuida se denomina así para describir las consecuencias que resultan de un

ataque desde varias máquinas. No es sorprendente que, para cualquier empresa en línea, un ataque de DDOS restrinja severamente su capacidad de mantener la disponibilidad de su servicio comercial.

III. Fraude en línea

Fraude en línea es un término amplio que abarca las transacciones en Internet que involucran información falsificada. Algunas de las formas más comunes de fraude en línea son la venta a través de Internet de documentos falsificados, tales como identificaciones falsas, diplomas y cartas de recomendación vendidas como documentos, ofertas de dinero fácil, tales como ofertas de trabajos en casa que prometen hacer ganar miles de dólares a las personas por hacer tareas triviales, llamadas en broma, en las que la conexión telefónica conduce a costosos cargos de larga distancia; y obras de beneficencia inexistentes, donde se solicitan donaciones para causas falsas.

Robo de identidad

El **robo de identidad** es una de las formas principales de fraude en línea o declaración falsa. El robo de la identidad personal en Internet es una de las formas más nuevas de fraude observadas en entornos tradicionales durante muchos años. Por ejemplo, en los entornos tradicionales, los ladrones abren cuentas de tarjetas de crédito con el nombre, la dirección y el número de seguridad social de una víctima o cuentas bancarias utilizando una identificación falsa. En el mundo en línea, la información de comercio electrónico puede ser interceptada como consecuencia de las vulnerabilidades de la seguridad informática. Los ladrones pueden tomar esta información (tal como números de tarjetas de crédito) y hacer con ella lo que deseen. Ésta es una de las razones por la que es de importancia fundamental que los consumidores y las organizaciones consigan las herramientas de seguridad informática apropiadas, que sirven para prevenir muchas de esas intercepciones.

El robo de identidad también se puede llevar a cabo en gran escala, como en el caso de una compañía o hasta una ciudad. Por ejemplo, en enero de 2001, la totalidad de la municipalidad de Largo, Florida perdió el servicio de correo electrónico durante más de una semana cuando una compañía desconocida con sede en España puso en peligro su identidad. La compañía incursionó ilegalmente en el sistema de retransmisión de correo electrónico de la ciudad para robar la identidad de Largo.com. Muy pronto, una avalancha de mensajes publicitarios (spam) de correo electrónico aparentemente provenientes de direcciones de Largo.com inundaron la red, y muchos Proveedores de Servicios de Internet pusieron en la lista negra a todos los mensajes electrónicos de entrada y salida de la ciudad.

Robo de datos

Robo de datos es el término que se utiliza para describir no sólo el robo de información, sino también la lectura o manipulación no autorizadas de la información privada. Los ejemplos de robo de datos abundan. En 1996, un joven británico de 16 años y un cómplice robaron mensajes con órdenes enviados por los comandantes a los pilotos en operaciones de batalla aérea desde el Laboratorio Rome de la Fuerza Aérea en Nueva York. Ambos también utilizaron las propias computadoras de la Fuerza Aérea

para obtener información del cuartel general de la OTAN y del Instituto de Investigación Atómica de Corea del Sur.

En abril de 2001, dos empleados de Cisco Systems fueron acusados de obtener acceso no autorizado a títulos de Cisco. Estas dos personas, que trabajaban en el departamento contable de la compañía, ingresaron al sistema informático que manejaba la distribución de títulos y pudieron transferir acciones a sus carteras de valores privadas. El valor total de sus acciones en dos intentos de transferencia por separado fue de aproximadamente $6,3 millones, según el Departamento de Justicia de Estados Unidos. Estos son unos cuantos ejemplos. Cualquiera, joven o anciano, esté dentro o fuera de una compañía, puede perturbar las actividades nacionales y comerciales poniendo así en peligro los sistemas.

Los gobiernos pueden ayudar a los usuarios a protegerse y deben dar el ejemplo.

Los gobiernos de todo el mundo se interesan cada vez más por la seguridad en línea, al reconocer la amenaza que representan los delitos en el ciberespacio para las empresas y las personas, así como a causa del crecimiento en Internet y el desarrollo del comercio electrónico.

La Unión Europea, por ejemplo, inició recientemente una amplia averiguación sobre la seguridad de la información y las redes. (Para ver los comentarios de BSA sobre esta averiguación, haga clic aquí).

Cuando desarrollan soluciones, las autoridades responsables deben recordar que la "confianza" en Internet y otras redes se basa en los siguientes fundamentos:

- *Seguridad*: confiar en que ningún tercero podrá obtener información del usuario mediante ataques de hackers u otro acceso no autorizado; y
- *Protección de datos personales*: confiar en que la información recopilada en forma legítima no sea utilizada en forma inesperada o imprevista.

Comprendidos estos conceptos, los gobiernos pueden realizar valiosos aportes para mejorar la confianza en línea cumpliendo con los importantes principios que aparecen a continuación:

- **Los gobiernos deben dar el ejemplo.**
- Al ser parte de los principales usuarios de tecnologías informáticas, los gobiernos deberán desempeñar un papel clave para asegurar su propia seguridad en el ciberespacio y, durante el proceso, dar el ejemplo a empresas y personas. El gobierno debe:
    - implantar políticas de administración atinadas y utilizar soluciones de vanguardia que garanticen la seguridad de sus propios sistemas informáticos,
    - fortalecer y armonizar las penas y los daños civiles contra delitos informáticos;
    - brindar recursos e instaurar incentivos para lograr una mejor investigación y desarrollo básicos de las tecnologías de seguridad;
    - alentar la capacitación de profesionales expertos en el campo de la seguridad informática; y
    - fomentar el aumento del intercambio de información y la difusión de las prácticas óptimas entre los sectores público y privado.

  Los gobiernos también pueden realizar un aporte importante en este área trabajando para lograr una consistencia internacional. Un gran número de organizaciones internacionales implementaron o están confeccionando declaraciones de principios o leyes modelo sobre importantes temas de seguridad. Un marco legal consistente en el ámbito internacional significa que los usuarios pueden confiar en la seguridad mientras recorran las redes.

  En este sentido, los gobiernos deben alentar el uso generalizado y voluntario de los Criterios Comunes, los cuales son un sistema de reconocimiento

internacional para definir los requisitos de seguridad de productos informáticos y de redes y evaluar si un producto en particular cumple con esos requisitos. Permiten que los usuarios realicen comparaciones valiosas con respecto a la seguridad ofrecida por los distintos productos.

- **La cooperación es esencial.** Encarar los desafíos de la protección de datos y la seguridad requiere de un esfuerzo conjunto de las industrias (como desarrolladoras de sistemas informáticos con los conocimientos y la pericia necesarios para su protección), de los gobiernos (con sus responsabilidades para lograr el bienestar público y fomentar el crecimiento económico), de los usuarios y de la aplicación de la ley.
- **La innovación conduce a las soluciones.** El mercado es el agente más apropiado para identificar y desarrollar soluciones de tecnología de vanguardia y garantizar que los consumidores cuenten con una amplia gama de opciones. Los gobiernos pueden colaborar con este proceso manteniendo una posición de neutralidad tecnológica, evitando imponer el uso de tecnologías o normas que retrasen la innovación.
- **La flexibilidad es la clave.** Como las soluciones de seguridad no constituyen una propuesta que se adapte a todas las necesidades, los gobiernos deben trabajar para garantizar que las empresas y las personas tengan flexibilidad para emplear las soluciones más eficaces a su alcance, y la libertad para evaluar considerando factores como: el nivel de amenazas, el costo y la facilidad de despliegue y uso.
- **La seguridad empieza con el usuario.** Las personas, las empresas y las entidades públicas pueden hacer mucho para proteger su propia información, desplegando tecnologías de protección de datos y seguridad eficaces y estableciendo criterios apropiados para la divulgación de la información. En la actualidad, las tecnologías como los dispositivos de autenticación, los programas antivirus, las herramientas de encriptación y los firewalls constituyen importantes medidas preventivas contra intromisiones no deseadas.

La tecnología faculta a las personas a protegerse por sí mismas.

La autoayuda es la primera y mejor línea de defensa contra intrusiones no deseadas en la red. Las personas, empresas y entidades públicas están mejor posicionadas para proteger su propia información. Las tecnologías de seguridad desarrolladas por la industria, incluyendo la encriptación (protección de datos electrónicos), las herramientas para autenticación (identificación de uno mismo en forma electrónica) y los firewalls (prevención de acceso no autorizado) constituyen herramientas poderosas para que los usuarios se protejan:

- **Encriptación**. Una de las mejores maneras de fomentar la seguridad y la protección de datos en las transacciones electrónicas es a través del uso de la encriptación. La encriptación permite que las personas codifiquen los archivos y mensajes privados, muy similar al modo en que una cerradura de combinación garantiza la protección de la privacidad de la información en un archivero. A menos que las personas confíen en que los mensajes electrónicos son plenamente seguros y privados, seguirán mostrándose renuentes a utilizar Internet u otras redes "abiertas" para enviar comunicaciones confidenciales.

  Sin embargo, para brindar una solución eficaz, la encriptación debe estar ampliamente disponible. Durante años, muchos gobiernos trataron de restringir la venta o el uso de poderosos productos de encriptación. Pero, como los delincuentes mantenían su capacidad de conseguir tecnología de encriptación, aunque en forma ilegal, las restricciones impuestas sobre la venta y el uso tuvieron un efecto perverso, al traer como consecuencia que las comunicaciones de los delincuentes fuesen más seguras que las de las empresas y los gobiernos.

  En reconocimiento de este hecho, los gobiernos se han movido para eliminar las restricciones excesivas en cuanto a la importación, el uso y la exportación de poderosas herramientas de encriptación. BSA apoyó plenamente las leyes de encriptación de Estados Unidos[1] que liberan los controles de encriptación, así como también las iniciativas de ley de productos de doble uso de la Unión Europea[1], ya que éstas promoverán la disponibilidad generalizada de la encriptación. Para obtener más información lea encriptación más abajo.

  Autenticación. Las firmas electrónicas permiten a las partes que celebran contratos en forma electrónica probar que la otra parte es la persona que asegura ser. Estas tecnologías ayudan a los usuarios en línea a establecer la identidad de la otra parte, verificar si se ha comprometido la integridad de un mensaje electrónico y cumplir con requisitos de firma que la ley pueda exigir en contratos u otros documentos. Se pueden utilizar diversas tecnologías para crear firmas electrónicas, incluyendo "tarjetas inteligentes", tecnologías biométricas, contraseñas, códigos, criptografía asimétrica y otras. BSA y sus miembros están a la vanguardia de estas tecnologías de autenticación.

  BSA respalda la legislación que da vigencia y extiende la aceptación de las firmas electrónicas. Como consecuencia de la diversidad de tecnologías disponibles, dichas leyes deben ser neutrales en cuanto a tecnología. BSA es una firme defensora de la Directiva de Firmas Electrónicas de la UE, que establece las reglas que gobiernan las firmas en línea. BSA también apoya enérgicamente

la Ley de FIRMA ELECTRÓNICA de EE.UU., que valida las firmas electrónicas en todo Estados Unidos de una forma que resulta neutral en cuanto a tecnología. Ver firmas electrónicas más abajo.

Protección antivirus. Las herramientas antivirus son indispensables para prestar a las personas la protección básica contra virus y otras formas de códigos informáticos maliciosos. Ante la ausencia de estas herramientas, los códigos maliciosos pueden causar graves daños en (o hasta la eliminación de) en los archivos, provocar la pérdida de la privacidad de la información personal o hasta destruir el disco duro de la computadora. Sin embargo, para que las soluciones antivirus brinden máxima protección, se deberán actualizar con frecuencia. Debido a su capacidad de conferir a las personas protección básica contra algunas de las formas más comunes de riesgos de la seguridad informática, las soluciones antivirus se han convertido en un componente básico de la seguridad en línea.

Firewalls. Un firewall es fundamentalmente un filtro que controla el acceso desde Internet a una red informática, bloqueando la entrada de las comunicaciones o los archivos no autorizados o potencialmente dañinos. Mediante el control del "tráfico" de Internet hacia una red, los firewalls protegen a las personas y las organizaciones contra intrusiones no deseadas, sin reducir la eficacia de las operaciones de las computadoras o las redes. También limitan las intrusiones a una parte de la red impidiendo que se dañen otras partes, por lo que ayudan a prevenir la paralización de sistemas de gran escala producidos por ataques en el ciberespacio. Entonces, no resulta sorprendente que los firewalls se hayan convertido en un componente clave de los sistemas informáticos actuales y que su arquitectura conste de la tecnología más novedosa disponible en el mercado actual.

La industria, a través del mercado, puede ir al frente de todos.

Debido a que las soluciones de seguridad no se adaptan a todas las necesidades, la industria trabaja en forma constante para asegurar que las empresas y las personas dispongan de las soluciones más eficaces. Los gobiernos deben desempeñar un papel importante para garantizar que las empresas y las personas tengan flexibilidad para utilizar las soluciones de su elección y la libertad para evaluarlas, a la luz de factores como el nivel de amenazas, el costo y la facilidad de despliegue y uso.

La flexibilidad es la clave, ya que las necesidades de seguridad a menudo varían según las situaciones y los usuarios específicos. Por ejemplo, los mecanismos de seguridad necesarios para proteger a una persona que compra un libro en línea pueden ser muy distintos de los de un banco que realiza una transacción en línea de $100 millones. Como la seguridad no es una propuesta que se adapte a todas las situaciones, los criterios como las normas de diseño "únicas" no tienen sentido. En cambio, BSA y sus compañías asociadas respaldan políticas públicas que continúan fomentando la innovación tecnológica y acrecientan las opciones de los consumidores.

Encriptación

La encriptación es la tecnología, ya sea hardware o software, para cifrar mensajes de correo electrónico, información de base de datos y otros datos informáticos, con el fin de mantenerlos confidenciales. Mediante el uso de ecuaciones matemáticas sofisticadas, la tecnología de encriptación moderna posibilita la protección de información confidencial con una cerradura electrónica a prueba de selección que impide a los ladrones, hackers, y espías industriales obtener información privada o personal de las personas, empresas y organismos del gobierno.

En algún momento, la encriptación pertenecía casi exclusivamente al ámbito de las agencias de inteligencia y el ejército. Pero con el auge de la tecnología informática y el uso de redes informáticas para compartir información y hacer negocios, se ha convertido en parte decisiva de la vida diaria para muchos estadounidenses.

La encriptación puede proteger información financiera y médica de carácter confidencial contra la divulgación no autorizada, salvaguardar las transacciones de comercio electrónico incluyendo los números de las tarjetas de crédito, mantener la confidencialidad de los negocios privados, y ayudar a que ambas partes de una transacción electrónica autentifiquen la identidad de la otra.

La encriptación potente también protege las redes informáticas vitales de EE.UU. e internacionales contra ataques de hackers y otros delincuentes, salvaguardando de ataques nuestro control de tráfico aéreo, la distribución de electricidad, el mercado financiero y los sistemas de telecomunicaciones . A medida que la economía norteamericana de la alta tecnología se expande, la encriptación se vuelve más importante para los intereses económicos, sociales y de seguridad nacional de los Estados Unidos. Una tecnología de encriptación sistemática en todo el mundo se traducirá en una Internet más perfecta y allanará el terreno para el comercio electrónico a escala global.

Durante el debate sobre las reglamentaciones de la encriptación, el Congreso estadounidense introdujo leyes : The SAFE Act in the House, (el proyecto de la Ley de Seguridad, en la Cámara de Representantes) patrocinada por los legisladores Bob Goodlatte (R-VA) y Zoe Lofgren (D-CA) y el proyecto de Ley de Protección, en el Senado, patrocinada por el senador John McCain, que hubieran eliminado las restricciones a la exportación. La votación de ambos proyectos legislativos estaba programada en el Congreso para el verano boreal de 1999, pero la misma fue postergada cuando el Gobierno de Bill Clinton se comprometió a tratar las preocupaciones de la industria. El apoyo inquebrantable del Congreso fue decisivo en el cambio de política para liberalizar los controles a la exportación.

Lea acerca de **Privacy and Security of Electronic Transactions** (PDF)

Comunicados de prensa sobre la encriptación

Haga clic aquí para explorar nuestros comunicados de prensa sobre la encriptación.

Para obtener más información, visite:
Americans for Computer Privacy (www.computerprivacy.org)

Richard Clarke Address (PDF, 82K)
BSA CEO Security Blueprint (PDF, 114K)
Are You Cyber Secure? (PDF, 472K)
CEO Letter to President Bush (PDF, 164K)
BSA Comments on EU Communication
BSA White Paper: Online Trust (PDF, 3.4 MB)

Firmas electrónicas

Recomendaciones de políticas

Asegurar la neutralidad tecnológica y la flexibilidad reguladora

Es fundamental que la legislación sobre firmas electrónicas sea tecnológicamente neutral y lo suficientemente flexible para dar cabida a los desarrollos futuros.

Fundamentos: Si bien aún es incipiente, el mercado de firmas electrónicas engloba una serie de tecnologías y procedimientos que permiten identificar y autenticar personas. Entre estos recursos se encuentran los números y contraseñas de identificación personal, las tarjetas o fichas inteligentes, la biométrica, los datos electrónicos simples, las firmas digitales (basadas en una infraestructura de "claves públicas") y distintas combinaciones de estas tecnologías. Aunque los productos que incorporan las tecnologías de firmas digitales actualmente tienen un alto impacto en el mercado, ciertas aplicaciones de esta tecnología pueden ser costosas y complejas a la hora de administrarlas.

Una legislación tecnológicamente neutral beneficiará tanto a los consumidores como a la industria. Un esquema regulador que sea impositivo u ofrezca ventajas legales o de otros tipos a determinadas tecnologías específicas "congelará" el avance tecnológico desalentando al sector industrial a invertir en productos y servicios de otro modo prometedores que no se adecuan al patrón regulador. Las verdaderas víctimas de una legislación tecnológicamente específica serían los consumidores, que jamás cosecharían los beneficios de productos mejorados y menos costosos que se habrían desarrollado en un entorno regulador más abierto.

Apoyar el desarrollo de normas técnicas impulsadas por el mercado

La legislación sobre firmas electrónicas no debe imponer normas obligatorias a productos de firmas electrónicas ni ampliar los beneficios legales sólo a normas "preferidas".

Fundamentos: Cierto grado de estandarización puede, efectivamente, beneficiar a los usuarios. Sin embargo, el sector de la tecnología de la información se ha destacado ampliamente en el desarrollo de normas técnicas y otras normas adecuadas a través de la elección del consumidor y el consenso de la industria. Estas normas impulsadas por el mercado responden totalmente a la demanda del consumidor, a la vez que brindan a la industria la flexibilidad para adaptarse rápidamente a las necesidades del usuario y los avances tecnológicos. Los normas técnicas obligatorias impuestas por el gobierno (en contraposición a las normas impulsadas por el mercado) no son necesarias, y probablemente sólo logren impedir el desarrollo tecnológico, distorsionar los mercados de productos de firmas electrónicas y perjudicar a los consumidores al restringir su capacidad de elección.

Permitir la libertad contractual con relación al uso de firmas electrónicas

La legislación sobre firmas electrónicas debe incorporar y respaldar expresamente el principio de libertad contractual entre partes privadas.

Fundamentos: Con toda la información a su disposición, las partes deben ser libres de establecer por contrato los términos y condiciones (incluyendo la elección de reglas legales y disposiciones de responsabilidad) según los cuales utilizarán y aceptarán las firmas electrónicas, ya sea para la celebración de contratos o para otros fines. La capacidad de modificar por contrato las normas sobre firmas electrónicas permitirá que las partes respondan a las necesidades y demandas del mercado, y de ese modo promoverá el crecimiento del comercio electrónico. Particularmente en el contexto de las transacciones internacionales, es fundamental que las partes sujetas a sistemas legales diferentes tengan la libertad de estructurar sus transacciones de la forma que mejor se adapte a las necesidades mutuamente convenidas.

No discriminar entre contratos en papel y contratos electrónicos

La legislación sobre firmas electrónicas debe garantizar en general que esas firmas electrónicas -y los contratos y registros a los que se adjuntan- no estén sujetas a reglas y requisitos más onerosos que los que se aplican a las firmas y contratos tradicionales.

Fundamentos: La imposición de más reglas o de reglas más estrictas sobre las firmas, contratos y registros electrónicos limitará el uso que hagan las partes del comercio electrónico, ya que tendrán una flexibilidad reducida con respecto a la forma de estructurar sus transacciones. La decisión de utilizar métodos electrónicos o de papel debe regirse por las necesidades o por las partes y no por diferencias artificiales incorporadas a las estructuras legales rectoras.

Dar prioridad a las leyes locales y regionales que imponen requisitos adicionales o que se contrapongan

Es necesario dar prioridad a las leyes locales y regionales que imponen requisitos que se agregan o entran en conflicto con aquellos impuestos por leyes nacionales, a fin de garantizar el desarrollo irrestricto del comercio electrónico.

Fundamentos: Las partes pretenderán celebrar contratos electrónicos desde diferentes lugares de un país, sin verse restringidas por barreras geográficas. Si dicha actividad debe crecer y prosperar, es necesario asegurar certeza y previsibilidad con relación a la validez y el cumplimiento de los contratos privados independientemente de las fronteras políticas internas. El comercio electrónico se verá entorpecido si las partes tienen que navegar por un laberinto de leyes locales y regionales inconsistentes e inadecuadas, problema que resulta agravado por la dificultad, en el entorno electrónico, de determinar la ubicación de la parte con la que se está celebrando el contrato. Una legislación sobre firmas electrónicas que no dé prioridad a las leyes locales y regionales sentaría las bases para varios regímenes legales locales y regionales con los que las partes deberían cumplir, lo cual elevaría los costos de transacción y tendría el potencial de que la celebración de contratos electrónicos resultase económicamente imposible en el caso de transacciones de poco valor.

Garantizar que todo esquema de licencia sea verdaderamente voluntario

Muchas empresas ya están desarrollando infraestructuras de firmas electrónicas fiables y sofisticadas exclusivamente en respuesta a la demanda del mercado. Sin embargo, si la legislación sobre firmas electrónicas incluye alguna forma de concesión de licencias,

es fundamental que el régimen sea totalmente voluntario y que a los proveedores con licencia no se les confieran beneficios legales ni de otros tipos que no se extiendan de igual manera a los proveedores sin licencia.

Fundamentos: Las firmas suministradas por proveedores sin licencia deben tener el mismo efecto legal que aquellas ofrecidas por proveedores con licencia. Si bien algunos consumidores valorarán el "sello" de aprobación gubernamental que podrían ofrecer los proveedores con licencia, exigir que todos los proveedores tengan licencia impondría costos agregados y cargas administrativas importantes. Lejos de beneficiar a los consumidores, un esquema de licencias obligatorio conllevaría sin duda que el comercio electrónico resultarse económicamente imposible para una amplia gama de transacciones de bajo costo y valor, erosionando así la confianza de los consumidores en dichas transacciones.

Ampliar el reconocimiento legal a certificados de uso limitado y sistemas cerrados

La legislación sobre firmas electrónicas debe extender el reconocimiento legal a las firmas electrónicas que están acompañadas de certificados de "uso limitado" o que se emplean en sistemas cerrados. Las leyes actuales sobre firmas electrónicas a menudo se centran en certificados de "identidad", diseñados para permitir que partes no relacionadas puedan establecer con certeza la identidad de la otra parte sobre la base exclusiva del certificado. Si bien los certificados de identidad pueden desempeñar un papel importante en el comercio electrónico futuro, la gran mayoría de los certificados que se usan hoy en día son certificados de uso limitado y sistemas cerrados. Esta tendencia tiene la apariencia de consolidarse en el futuro inmediato.

Fundamentos: Los certificados de uso limitado, a diferencia de los certificados de identidad, no se emplean para transacciones generales con personas y entidades no relacionadas; más bien, están diseñados para contextos limitados específicos en los cuales el signatario y el receptor tienen una relación preexistente. De esta forma, ambas partes son totalmente conscientes del alcance y uso limitados de dichos certificados. Los certificados de sistemas cerrados representan un tipo específico de certificado de uso limitado en el cual el certificado está limitado no sólo por la naturaleza de la transacción sino también por el sistema en el cual éste se puede usar. Al igual que los certificados de uso limitado, los certificados de sistemas cerrados reflejan la afiliación del signatario en un grupo predefinido y generalmente permiten que el signatario acceda a información, utilice servicios o participe de transacciones sobre la base de una relación preexistente. Los certificados de uso limitado y los de sistemas cerrados se pueden emplear para distintos fines, por ejemplo, para verificar el estado de empleo del titular en una empresa, corroborar la afiliación a una organización o confirmar electrónicamente el acceso de una estación de trabajo a una red.

Dado que los certificados de sistemas cerrados y uso limitado constituirán algunos de los elementos más comunes e importantes en el comercio electrónico, es fundamental que dichos certificados sean reconocidos como legalmente válidos y admitidos como pruebas en procesos legales.

Ampliar el reconocimiento legal a agentes electrónicos

La legislación sobre firmas electrónicas debe abarcar las firmas generadas por agentes electrónicos, es decir, por programas informáticos que inician o responden a mensajes sin la intervención humana contemporánea, en transacciones de negocio a negocio (B2B).

Fundamentos: Los agentes electrónicos ya se usan ampliamente en sistemas en los que realizan transacciones en nombre de sus mandantes, quienes crearon dichos agentes y los autorizaron para actuar en su nombre (por ejemplo, en sistemas de intercambio de datos y proveedores en línea. A medida que crece el comercio electrónico, se espera que el uso de los agentes electrónicos sea cada vez más frecuente en el mundo de los negocios, ya que promueven la práctica más eficiente del comercio en línea. En este contexto, para que el comercio electrónico desarrolle todo su potencial, las firmas electrónicas generadas por los agentes electrónicos deben tener el mismo efecto legal que las firmas electrónicas generadas por los propios mandantes.

Permitir que los signatarios firmen en forma electrónica por sí mismos o en nombre de entidades legales.

La legislación de firmas electrónicas debe garantizar que un signatario pueda firmar electrónicamente no sólo en su nombre sino también en el de una entidad legal a la que esté autorizado a representar, tal como una corporación o sociedad.

Fundamentos: Las firmas electrónicas se usan más comúnmente en transacciones en las que participan organizaciones, empresas y otras entidades legales. Es probable que esta tendencia continúe en el futuro. Por lo tanto, los signatarios deberían estar autorizados a firmar documentos electrónicamente en nombre de entidades legales, como actualmente pueden hacerlo en documentos firmados manualmente.

Reconocer la validez de las firmas electrónicas de otros países

Por último, la legislación sobre firmas electrónicas debe garantizar que cualquier marco legal que se adopte sea totalmente compatible con las normas internacionales y no discrimine las firmas electrónicas de otros países.

Fundamentos: El comercio electrónico es por su propia naturaleza global. Por lo tanto; es fundamental que las estructuras reguladoras reconozcan la validez legal de las firmas electrónicas que se originan en otros países. Una serie de organismos internacionales (como UNCITRAL) actualmente está trabajando en leyes modelo sobre firmas electrónicas. Muchos países están preparando legislación al respecto, otros ya la adoptaron. A fin de asegurar que los consumidores y las empresas tengan la mayor cantidad de opciones para participar en comercio electrónico con partes de otros países, cualquier legislación sobre firmas electrónicas debe ofrecer un marco legal abierto y flexible que permita razonablemente el reconocimiento de las firmas electrónicas que se originen en otros países.