Seguridad Informática

Desde la consolidación de Internet como medio de interconexión global, los incidentes de seguridad relacionados con sistemas informáticos vienen incrementándose de manera alarmante. Este hecho, unido a la progresiva dependencia de la mayoría de organizaciones hacia sus sistemas de información, viene provocando una creciente necesidad de implantar mecanismos de protección que reduzcan al mínimo los riesgos asociados a los incidentes de seguridad. En este artículo, vamos a proporcionar una visión general de los aspectos más relevantes de la seguridad informática, observando esta disciplina desde un punto de vista estratégico y táctico. Para ello destacaremos la conveniencia de afrontar su análisis mediante una aproximación de gestión, concretamente con un enfoque de gestión del riesgo. Para completar esta visión introductoria a la seguridad informática, mencionaremos las amenazas y las contramedidas más frecuentes que deberían considerarse en toda organización.

Introducción

La seguridad informática, de igual forma a como sucede con la seguridad aplicada a otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada. Esta visión de la seguridad informática implica la necesidad de gestión, fundamentalmente gestión del riesgo. Para ello, se deben evaluar y cuantificar los bienes a proteger, y en función de estos análisis, implantar medidas preventivas y correctivas que eliminen los riegos asociados o que los reduzcan hasta niveles manejables.

En general cualquier persona consideraría poco razonable contratar a un agente de seguridad en exclusiva para proteger su domicilio. Posiblemente sería una medida de seguridad excelente para evitar accesos no autorizados a nuestro domicilio, sin embargo, muy pocos lo considerarían, simplemente por motivos económicos. Tras evaluar el valor de los bienes a proteger, lo habitual sería considerar otras medidas más acordes con el valor de nuestros bienes. Podríamos pensar en una puerta blindada, un conserje compartido con otros vecinos o incluso un servicio de vigilancia privada basada en sensores, alarmas y acceso telefónico con una central de seguridad. Combinando estas medidas preventivas con otras correctivas como podría ser una póliza de seguro contra robo, alcanzaríamos un nivel de seguridad que podría considerarse adecuado. Muchas veces sin hacerlo de forma explícita, habríamos evaluado el valor de nuestros bienes, los riesgos, el coste de las medidas de seguridad disponibles en el mercado y el nivel de protección que ofrecen.

En seguridad informática, los principios mostrados con nuestro ejemplo de seguridad en el domicilio son igualmente aplicables. Las únicas diferencias aparecen por las particularidades técnicas asociadas a los sistemas informáticos. La valoración económica de los bienes a proteger puede ser muchas veces una tarea compleja, la casuística de los riesgos potenciales muy grande, y la complejidad y diversidad de las medidas de seguridad disponibles dificulta su selección. Sin embargo, el fondo sigue siendo el mismo, seguridad implica proteger alguna entidad frente a un conjunto de riesgos y en este caso riesgos relacionados con los sistemas informáticos.

En este artículo vamos a dar una visión general a los aspectos más relevantes de la seguridad informática, comenzando con una visión de la seguridad como parte integral de la gestión empresarial, continuaremos con la descripción de las amenazas más frecuentes que pueden comprometer los sistemas informáticos y con la descripción de las medidas más efectivas para contrarrestarlas. Por último, finalizaremos mencionando las actividades más significativas que venimos realizando en el Instituto Tecnológico de Informática en materia de seguridad.

Objetivos de la Seguridad Informática

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la seguridad informática ayuda a la organización cumplir sus objetivos, protegiendo sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como inmateriales. Desafortunadamente, en ocasiones se ve a la seguridad informática como algo que dificulta la consecución de los propios objetivos de la organización, imponiendo normas y procedimientos rígidos a los usuarios, a los sistemas y a los gestores. Sin embargo debe verse a la seguridad informática, no como un objetivo en sí mismo, sino como un medio de apoyo a la consecución de los objetivos de la organización.

En general el principal objetivo de las empresas, es obtener beneficios y el de las organizaciones públicas, ofrecer un servicio eficiente y de calidad a los usuarios. En las empresas privadas, la seguridad informática debería apoyar la consecución de beneficios. Para ello se deben proteger los sistemas para evitar las potenciales pérdidas que podrían ocasionar la degradación de su funcionalidad o el acceso a los sistemas por parte de personas no autorizadas. De igual forma, las organizaciones públicas deben proteger sus sistemas para garantizar la oferta de sus servicios de forma eficiente y correcta.

En cualquier caso, los gestores de las diferentes organizaciones deberían considerar los objetivos de la propia organización e incorporar la seguridad de los sistemas desde un punto de vista amplio, como un medio con el que gestionar los riesgos que pueden

comprometer la consecución de los propios objetivos, donde la cuantificación de los diferentes aspectos, muchas veces económica, debe ser central.

Gestión del Riesgo

La protección de los sistemas y de la información no suele eliminar completamente la posibilidad de que estos bienes sufran daños. En consecuencia, los gestores deben implantar aquellas medidas de seguridad que lleven los riesgos hasta niveles aceptables, contando para ello con el coste de las medidas a implantar, con el valor de los bienes a proteger y con la cuantificación de las pérdidas que podrían derivarse de la aparición de determinado incidente de seguridad.

Los costes y beneficios de la seguridad deberían observarse cuidadosamente para asegurar que el coste de las medidas de seguridad no excedan los beneficios potenciales. La seguridad debe ser apropiada y proporcionada al valor de los sistemas, al grado de dependencia de la organización a sus servicios y a la probabilidad y dimensión de los daños potenciales. Los requerimientos de seguridad variarán por tanto, dependiendo de cada organización y de cada sistema en particular.

En cualquier caso, la seguridad informática exige habilidad para gestionar los riesgos de forma adecuada. Invirtiendo en medidas de seguridad, las organizaciones pueden reducir la frecuencia y la severidad de las pérdidas relacionadas con violaciones de la seguridad en sus sistemas. Por ejemplo, una empresa puede estimar que está sufriendo pérdidas debidas a la manipulación fraudulenta de sus sistemas informáticos de inventariado, de contabilidad o de facturación. En este caso puede que ciertas medidas que mejoren los controles de acceso, reduzcan las pérdidas de forma significativa.

Las organizaciones que implantan medidas adecuadas de seguridad, pueden obtener un conjunto de beneficios indirectos que también deberían considerarse. Por ejemplo, una organización que cuente con sistemas de seguridad avanzados, puede desviar la atención de potenciales intrusos hacia víctimas menos protegidas, puede reducir la frecuencia de aparición de virus, puede generar una mejor percepción de los empleados y otros colaboradores hacia la propia empresa, aumentando la productividad y generando empatía de los empleados hacia los objetivos organizativos.

Sin embargo, los beneficios que pueden obtenerse con medidas de seguridad presentan costes tanto directos como indirectos. Los costes directos suelen ser sencillos de evaluar, incluyendo la compra, instalación y administración de las medidas de seguridad. Por su parte pueden observarse costes indirectos, como decremento en el rendimiento de los sistemas, pueden aparecer necesidades formativas nuevas para la plantilla o incluso determinadas medidas, como un excesivo celo en los controles, pueden minar la moral de los empleados.

En muchos casos los costes asociados a las medidas de seguridad pueden exceder a los beneficios esperados por su implantación, en cuyo caso una correcta gestión llevaría a platearse su adopción frente a la posibilidad de simplemente tolerar el problema.

Amenazas

Los sistemas informáticos son vulnerables a multitud de amenazas que pueden ocasionar daños que resulten en pérdidas significativas. Los daños pueden variar desde simples errores en el uso de aplicaciones de gestión que comprometan la integridad de los datos, hasta catástrofes que inutilicen la totalidad de los sistemas. Las pérdidas pueden aparecer por la actividad de intrusos externos a la organización, por accesos fraudulentos, por accesos no autorizados, por el uso erróneo de los sistemas por parte de empleados propios, o por la aparición de eventualidades en general destructivas.

Los efectos de las diversas amenazas puedes ser muy variados. Unos pueden comprometer la integridad de la información o de los sistemas, otros pueden degradar la disponibilidad de los servicios y otros pueden estar relacionados con la confidencialidad de la información. En cualquier caso una correcta gestión de los riesgos debe implicar un profundo conocimiento de las vulnerabilidades de los sistemas y de las amenazas que los pueden explotar. Las propias características de las organizaciones deben influir en las medidas de seguridad que resulten más adecuadas y más eficientes en términos de costes, para contrarrestar las amenazas o incluso para tolerarlas conociendo en todo caso sus implicaciones.

A continuación vamos a mostrar las amenazas más frecuentes que deberían ser tenidas en cuenta por toda organización como fuentes potenciales de pérdidas. Conviene destacar que la importancia de una u otra amenaza varía de forma significativa entre organizaciones distintas y que debería hacerse un estudio individualizado de sus repercusiones concretas y de la probabilidad de su aparición.

1. Errores y omisiones

Los errores de los empleados al utilizar los sistemas pueden comprometer la integridad de la información que maneja la organización. Ni siquiera las aplicaciones más sofisticadas están libres de este tipo de problemas, que pueden reducirse con refuerzos en controles de integridad de los datos y con un adiestramiento adecuado del personal.

Muchas veces, simples errores pueden comprometer no únicamente la integridad de los datos, sino incluso puede que causen la aparición de nuevas vulnerabilidades en los sistemas. Este tipo de amenazas es si cabe más relevante en las empresas que se dedican al sector de las nuevas tecnologías, desarrollando e implantando sistemas, muchas veces interconectados entre diversas organizaciones. Un simple error de programación, en la administración, o la carencia de la formación necesaria para evaluar las implicaciones de seguridad de determinada aproximación de desarrollo, puede causar vulnerabilidades que afecten no únicamente a las organizaciones usuarias de los sistemas, sino también a las propias empresas que los desarrollan que se podrían ver muy perjudicadas en su imagen corporativa.

2. Intrusiones

Bajo esta amenaza se incluyen tanto actividades claramente fraudulentas, como meras intrusiones efectuadas por determinados individuos con el único fin de probar sus “habilidades” o incluso actos de sabotaje, terrorismo informático o espionaje industrial. Las actividades fraudulentas, incluido el robo, puede que sean las más preocupantes para muchas organizaciones, sobre todo para aquellas que tengan bienes de elevado valor, gestionados mediante sistemas informáticos. Ejemplos de este tipo de organizaciones pueden ser las entidades financieras, los organismos públicos que generen acreditaciones oficiales o incluso empresas de distribución o comercio electrónico, donde los sistemas informáticos pueden ser

susceptibles de alteración malintencionada con objeto de obtener provecho económico.

Los autores de las intrusiones pueden ser tanto externos a la propia organización, como internos. Es reseñable destacar que muchos estudios sobre fraudes y robos mediante tecnologías de la información coinciden en señalar que la mayoría de las actividades fraudulentas son realizadas por personal vinculado a la propia organización. Pueden ser empleados con acceso a sistemas o información no controlada, antiguos empleados con conocimientos tanto de los sistemas como de las medidas de seguridad internas o personas vinculadas en cierta forma con la organización y que gozan de determinados privilegios que muchas veces se esconden bajo aparentes relaciones cordiales con la propia empresa.

En muchos casos las intrusiones generan importantes daños económicos, pero en todos los casos causan una importante sensación de desprotección en toda la organización, que se agrava si no es posible identificar a los autores de las intrusiones, las técnicas empleadas para cometerlas o los objetivos que persiguen.

La creciente importancia de las intrusiones maliciosas en los sistemas informáticos la podemos encontrar reflejada en el siguiente

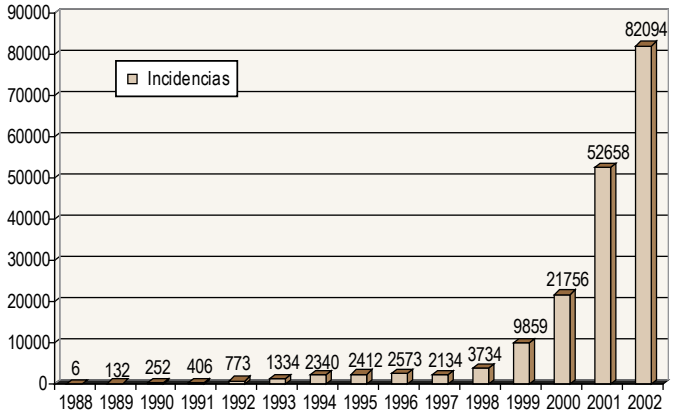

Figura 1: Evolución de las incidencias intervenidas por el CERT/CC (fuente: www.cert.org).

gráfico, donde se puede observar el alarmante incremento de incidentes de seguridad ocurrido en los últimos años.

Concretamente el gráfico muestra el número de incidentes ocasionados por intrusiones, y comunicados al *CERT,* un organismo de reconocido prestigio internacional dedicado a la prevención y análisis de los incidentes de seguridad aparecidos en Internet. Conviene destacar que las cifras únicamente muestran los datos comunicados al CERT, y que vienen a representar a las intrusiones efectuadas por parte de individuos externos a las propias organizaciones. Los datos se refieren a todo el mundo, sin embargo también destacamos que las cifras provienen mayoritariamente de grandes empresas, asentadas fundamentalmente en los Estados Unidos, Europa y Japón. Sin embargo, pese a lo parcial de las cifras, no deja de resultar ilustrativa la curva de crecimiento y las magnitudes de los incidentes constatados.

3. Accidentes y desastres

Eventualidades tan cotidianas como la simple rotura de una cañería, la pérdida de fluido eléctrico o la rotura de equipos o mecanismos de comunicaciones pueden tener efectos claramente negativos sobre los sistemas de información. Debe incluso contemplarse la posibilidad de aparición de eventos más graves, como incendios, atentados terroristas, inundaciones causadas por la propia naturaleza, tormentas eléctricas o actividades reivindicativas descontroladas de determinados colectivos.

4. Lógica maliciosa

Entre estas amenazas encontramos los virus, los gusanos, los caballos de Troya y las bombas lógicas. Aun existiendo diferencias técnicas entre ellas, el nexo común a todas estas amenazas consiste en que se trata de software creado en general para causar daño. Los costes asociados a su aparición pueden ser significativos y varían en función de la virulencia de sus acciones. Pueden suponer simplemente pérdidas debidas a la dedicación de personal y recursos a su eliminación o pérdidas mucho mayores si resultan afectados, corrompidos o destruidos sistemas críticos para la organización.

5. Amenazas a la privacidad de las personas

La acumulación de enormes cantidades de datos de carácter personal por entidades públicas y privadas, unida a la capacidad de los sistemas informáticos para combinar y procesar las informaciones vienen generando claras amenazas a la privacidad de los individuos. La constatación de estas amenazas por parte de la mayoría de países ha llevado a la elaboración de leyes y normas que limitan el tratamiento de los datos de carácter personal.

Estas amenazas no sólo afectan a los individuos, sino también a toda organización que manipule información sensible de personas. De no observarse la legislación vigente y en caso de no implantar las medidas adecuadas para su cumplimiento, se pueden derivar pérdidas, tanto económicas por las correspondientes multas, como de imagen corporativa.

Medidas de Seguridad

Existe un gran abanico de medidas de seguridad que pueden reducir el riesgo de pérdidas debidas a la aparición de incidentes en los sistemas informáticos. Muchas veces al hablar de medidas de seguridad, solo se mencionan las meramente técnicas, como cortafuegos, antivirus o sistemas de copias de respaldo. Sin embargo, las medidas más efectivas suelen ser las medidas de gestión planteadas a medio y largo plazo desde un punto de vista estratégico y táctico.

A continuación mencionaremos brevemente las medidas y sistemas de seguridad más frecuentes agrupándolas bajo dos aspectos. Medidas de gestión y medidas técnicas. Las primeras deben ser implantadas por los gestores de las organizaciones como parte de los planes estratégicos y tácticos, mientras que las segundas se corresponden con herramientas y sistemas técnicos diseñados para evitar, controlar o recuperar los daños que pueden sufrir los sistemas por la aparición de determinadas amenazas de seguridad.

1. Medidas de gestión

Los gestores de toda organización deberían contemplar la seguridad informática como parte integral de las estrategias y tácticas corporativas. Una vez plasmada la importancia de los sistemas para la consecución de los propios objetivos y los riesgos que puede suponer para la empresa la pérdida de integridad de su información, la indisponibilidad de sus sistemas o la violación de la confidencialidad

de su información, pueden plantearse con mayor rigor el resto de medidas encaminadas a servir a los objetivos empresariales.

Emanando de la vertiente estratégica de la información y de los sistemas corporativos, suelen generarse dos herramientas de gestión no menos importantes: las políticas de seguridad y el plan de contingencia.

Las políticas de seguridad de una organización son las normas y procedimientos internos que deben seguir los integrantes de la organización para respetar los requerimientos de seguridad que deseen preservarse. Debe describirse la criticidad de los sistemas y de la información, los roles de cada puesto de trabajo y la mecánica de acceso a los sistemas, herramientas, documentación y cualquier otra componente del sistema de información. Resulta frecuente desglosar las políticas de seguridad en procedimientos detallados para cada componente del sistema de forma individualizada, así por ejemplo, pueden crearse documentos que describan las políticas de tratamiento de correos electrónicos, políticas de uso de Internet, de copias de respaldo, de tratamiento de virus y otra lógica maliciosa, políticas formativas en materia de seguridad para la plantilla, etc. Conviene destacar que las políticas de seguridad deben emanar de la estrategia corporativa y que se trata de documentos que deberían conocer todos los integrantes de la plantilla.

Por su parte, el plan de contingencia describe los procedimientos que deben seguirse ante la aparición de eventualidades significativas que puedan suponer graves consecuencias para la organización. Debe detallarse los pasos a seguir, por ejemplo en caso de destrucción total de los sistemas por inundación, fuego, etc. Muchas veces la simple elaboración del plan descubre defectos en los sistemas que pueden ser paliados con relativa facilidad. Por ejemplo puede descubrirse que no se mantienen copias de respaldo de información crucial para la empresa en lugares físicamente seguros, o al menos en lugares distantes a la ubicación de los sistemas susceptibles de daños.

2. Medidas técnicas

Existen innumerables herramientas y sistemas de seguridad orientadas a preservar la integridad, confidencialidad y disponibilidad de información y sistemas. La oferta en este sentido es muy numerosa y toda organización debería dedicar un esfuerzo significativo a su estudio y selección. En este breve artículo, más que describir con detalle todas las herramientas y medidas de seguridad aplicables y sus variaciones disponibles en el mercado, nos limitaremos a mencionar las técnicas más utilizadas, apuntando finalmente algunas de las más novedosas.

Entre las técnicas más consolidadas encontramos las copias de respaldo, los antivirus, los cortafuegos, los mecanismos de autenticación y la criptografía. Las copias de respaldo y en general cualquier forma de redundancia, se encaminan a garantizar la disponibilidad de los sistemas frente a cualquier eventualidad.

Los antivirus pretenden evitar la aparición de lógica maliciosa y en caso de infección tratan de eliminarla de los sistemas. Entre los antivirus conviene destacar aquellos que inspeccionan los correos electrónicos evitando la infección de sus destinatarios. Por su parte, los cortafuegos tratan de reducir el número de vías potenciales de acceso a los sistemas corporativos desde el exterior, estableciendo limitaciones al número de equipos y de servicios visibles. Otra de las técnicas imprescindibles en toda organización la forman los mecanismos de autenticación. Estos mecanismos pueden variar desde esquemas simples basados en los pares usuario contraseña, hasta complejos sistemas distribuidos basados en credenciales o sistemas de autenticación biométricos basados en el reconocimiento mecanizado de características físicas de las personas. Por último, todo esquema de seguridad debe contemplar en una u otra medida el cifrado de información sensible. A veces puede ser suficiente el cifrado de las contraseñas, mientras que en otras resulta imprescindible el cifrado de las comunicaciones y de las bases de datos.

Como medidas más avanzadas, podemos mencionar la esteganografía, la detección de vulnerabilidades y la detección de intrusos. Las técnicas esteganográficas tratan de ocultar información. A diferencia de la criptografía, que trata de hacer indescifrable la información, la esteganografía trata de evitar que siquiera se note su existencia. Por ejemplo las empresas dedicadas a producir documentos digitales, pueden estar interesadas en incluir determinada marca invisible de forma que sea demostrable su autoría y puedan perseguirse copias ilegales.

Las herramientas de detección de vulnerabilidades suelen verse como herramientas de auditoria, que pueden mostrar las vías que con mayor probabilidad utilizarían los intrusos para acceder a los sistemas. Por último, los sistemas de detección de intrusos tratan de descubrir, muchas veces en tiempo real, accesos no autorizados a los sistemas, tanto desde el exterior de la organización, como desde dentro de las propias instalaciones de la empresa.

Seguridad en el Instituto Tecnológico de Informática

El área de Sistemas Fiables del Instituto Tecnológico de Informática, centra su trabajo en la investigación y desarrollo de entornos orientados a aumentar la fiabilidad y la disponibilidad, donde la seguridad informática se plantea como uno de los ejes fundamentales.

En esta área vienen realizándose proyectos de consultoría y auditoría de seguridad informática, cubriéndose los aspectos estratégicos, tácticos y técnicos de los sistemas informáticos. El objetivo de estos proyectos consiste en la elaboración de un procedimiento de consultoría utilizable por terceras empresas consultoras.

Además de la consultoría, se están desarrollando diversos proyectos de investigación y desarrollo, entre los que destacan IntruDec y TigerWeb. El primero consiste en un sistema de detección de intrusos basado en el reconocimiento de patrones de conducta sospechosos, observables al analizar el tráfico en la red y al analizar la actividad de los equipos informáticos. Por su parte, TigerWeb es una herramienta de detección de vulnerabilidades perimetrales. Con esta herramienta se puede obtener una visión aproximada de las vías más fácilmente explotables por potenciales intrusos para acceder a los sistemas desde el exterior de la organización.

Por último, el grupo de Sistemas Fiables también se encuentra inmerso en la investigación de las implicaciones de seguridad que tiene el empleo de sistemas inalámbricos y móviles, estudiando entre otros los mecanismos de autenticación, cifrado, encaminamiento y las arquitecturas software más convenientes donde se contemple la seguridad desde el punto de vista particular de este tipo de entornos.

Autor: Pablo Galdámez
Para más información sobre Seguridad Informática:
seguridad@iti.upv.es