

Monográfico

El reto de la ciberseguridad

Ciberseguridad: nuevas amenazas, nuevas estrategias

En este artículo, el profesor Villagrà hace un repaso histórico de la evolución del concepto de ciberseguridad desde la invención de Internet hasta el momento actual, de madurez en el ámbito de la seguridad en Internet. Analiza la evolución de las amenazas y los diferentes enfoques para la puesta en marcha de estrategias de seguridad efectivas.

Antecedentes históricos

El diseño y despliegue masivo de redes de telecomunicación ha permitido su utilización a gran escala, convirtiéndose en piezas claves para el funcionamiento de empresas y administraciones. Hoy, muchas personas ya no pueden imaginar una sociedad sin teléfonos móviles o Internet. La penetración social, comercial e industrial que están teniendo estas tecnologías ha hecho, a su vez, que se consideren como un medio potencial para la transmisión de ataques contra sus usuarios, sistemas de información e incluso contra sistemas de control interconectados a través de estas redes.

Si bien en las redes tradicionales de telefonía este tipo de incidentes no es muy frecuente, la versatilidad de las redes abiertas de comunicación de datos hace que sea mucho más sencillo para los atacantes encontrar mecanismos en dichas redes que permitan llevar a cabo ataques. Aunque la existencia de riesgos e incidentes ha estado presente en muchos entornos de comunicaciones de datos, el caso más significativo actualmente es el entorno de Internet, debido a su volumen, expansión y penetración social, comercial e industrial actualmente.

Los mecanismos básicos en los que se fundamenta Internet fueron diseñados durante las décadas de 1970 y 1980 con el objetivo principal de intercomunicar centros



Víctor A. Villagrà

Profesor Titular. Dpto. Ingeniería Telemática. E.T.S. Ingenieros Telecomunicación. Universidad Politécnica de Madrid.

[in.es.linkedin.com/in/victorvillagra](https://es.linkedin.com/in/victorvillagra)

de investigación y universidades. Este diseño no se realizó en absoluto pensando en una situación como la actual, de uso multidisciplinar a nivel global, sino que se realizó desde el punto de vista de una utilización en entornos mucho más restringidos y sobre todo, con usuarios con cierto nivel técnico y desde luego, no hostiles. Esto provocó que las tecnologías de seguridad que se incluyeron en los protocolos y servicios básicos fueran muy limitadas o incluso inexistentes. A día de hoy, muchos protocolos y servicios que usamos habitualmente son los diseñados originalmente, y cuya utilización directa implicaría graves riesgos de seguridad (por ejemplo, la transmisión en claro de las claves de los usuarios por las redes a la hora de descargar un correo electrónico), por lo que ha sido necesario añadir capas por encima que les dote de seguridad, manteniendo la interoperabilidad necesaria.

El 2 de noviembre de 1988, Robert Morris Jr., un estudiante de doctorado de informática de Cornell, desarrolló un programa experimental que aprovechaba una de las múltiples vulnerabilidades de los sistemas de comunicación para autorreplicarse y autopropagarse a sistemas vecinos a través de Internet. Lo lanzó desde el MIT (Massachusetts Institute of Technology), y rápidamente descubrió que se replicaba e infectaba las máquinas a una velocidad mucho mayor de lo que él esperaba, provocando la indisponibilidad de una gran cantidad de ordenadores, incluyendo universidades, organismos militares e institutos de investigación médica. Este ataque, denominado el "Gusano de Internet (*Internet Worm*)", fue la primera gran prueba de la falta de seguridad en la implantación de los mecanismos básicos y protocolos de Internet, pero ya era demasiado tarde para rediseñarlo de nuevo. Desde entonces, se han descubierto nuevas vulnerabilidades sobre todo en las aplicaciones que implementan los distintos protocolos y servicios de Internet, y ha sido necesario desarrollar nuevos parches para cubrir dichas deficiencias; algunos ataques llegaron a tener gran repercusión mediática, como por ejemplo MELISSA / ILOVEYOU (1999-2000, infección por adjunto de correo electrónico), RED CODE (2001, infección de los servidores Web IIS de Microsoft), BLASTER / SASSER (2003-2004, vulnerabilidad de Microsoft Windows), Conficker (2008, uno

de los más sofisticados empleando múltiples mecanismos simultáneamente).

Ante estos hechos, ha sido necesario el desarrollo de tecnologías especializadas en la seguridad en estas redes de telecomunicación, destinadas a proteger a sus sistemas frente a diversos tipos de ataques, permitiendo el despliegue de arquitecturas de seguridad en red que facilitan su uso de una forma más segura y confiable. Igualmente, el desarrollo de los programas es mucho más robusto y el ritmo de aparición de vulnerabilidades en programas ha decrecido bastante. Sin embargo, el entorno de los atacantes en Internet también ha evolucionado: si al principio los atacantes buscaban principalmente una relevancia mediática, actualmente los atacantes se mueven por otro tipo de motivaciones más cercanas a la delincuencia tradicional: se buscan beneficios económicos y/o estratégicos a nivel industrial. Por ello, los ataques no buscan un impacto global, sino que están dirigidos específicamente hacia un objetivo: son las denominadas Amenazas Persistentes y Avanzadas (Advanced Persistent Threats, APT).

Evolución de la amenaza

La identificación de fallos y vulnerabilidades en software, servicios y protocolos de Internet no es una tarea sencilla: sólo está al alcance de verdaderos expertos que controlan diversas disciplinas relacionadas (sistemas operativos, lenguajes de programación de bajo nivel, protocolos de red, etc.), un perfil conocido como “*hacker*”, el cual no tiene por qué estar asociado a actividades delictivas o dañinas, como recoge la controvertida acepción de dicho término en el Diccionario de la Real Academia de la Lengua (“pirata informático: persona con grandes habilidades en el manejo de ordenadores, que utiliza sus conocimientos para acceder ilegalmente a sistemas o redes ajenos”).

Este tipo de experto no es numeroso: se necesitan profundos conocimientos en múltiples disciplinas para descubrir vulnerabilidades en sistemas que afecten a su seguridad. Por ello, el conjunto de atacantes debería ser teóricamente reducido y potencialmente controlable. El problema surge cuando estos expertos deciden en un momento dado publicitar sus descubrimientos en Internet, muchas veces incluso sin informar a las compañías de *software* cuyos productos son, de repente, vulnerables, llegando en ocasiones a proporcionar métodos fáciles de utilizar (los programas denominados “*exploits*”), que cualquiera puede descargarse y utilizar para aprovecharse de la vulnerabilidad descubierta.



Aquí surge el verdadero problema de las amenazas de Internet. Se ponen a disposición de todo el mundo las armas con las que se pueden atacar los sistemas informáticos. No es necesario un elevado conocimiento técnico para poderlas utilizar, por lo que diversos sectores que no tienen una madurez suficiente en la utilización correcta de las tecnologías pueden usarlas indiscriminadamente sin tener conciencia de las posibles consecuencias. En este entorno surgieron distintos perfiles de atacantes de Internet:

- Durante muchos años, los atacantes no buscaban directamente un beneficio económico, sino más bien una relevancia mediática, o se correspondían con el perfil a veces etiquetado como “*hacker romántico*”: realiza ataques sólo para demostrarse que es capaz de hacerlo, o creyendo que está haciendo un favor al propietario del sistema atacado. Una vez ejecutado el ataque (normalmente, entrar sin autorización en algún sistema), no va más allá.



- ▶ En menor medida, se daba también el perfil del “*vándalo informático*”: causa deliberadamente destrozos y daños en la máquina atacada, frecuentemente buscando una relevancia mediática en sus ataques. Este ataque podemos verlo también en la actualidad en los denominados “*website defacements*”: un ataque a un servidor web que únicamente cambia la apariencia de dicho servidor web, con el fin de tener una relevancia mediática y poder transmitir reivindicaciones políticas o sociales.
- ▶ En los últimos años, los atacantes han evolucionado para conseguir un beneficio económico o estratégico. Para ello, tienen varias vías, entre las que destacan:
 - Son verdaderos expertos que descubren nuevas vulnerabilidades no conocidas. Son las denominadas *vulnerabilidades de día 0*, de las que pueden sacar grandes beneficios económicos, vendiéndolas a los fabricantes o en el mercado negro
 - Utilizan vulnerabilidades de día 0 compradas, o vulnerabilidades ya conocidas para realizar ataques e intentar lograr un beneficio económico de ello. Para ello, los atacantes deben organizar una campaña, usualmente en múltiples pasos, para lograr que la víctima sea objeto del ataque. Se valen habitualmente de técnicas de engaño a usuarios (usualmente conocidas como técnicas de ingeniería social) para lograr la colaboración involuntaria de los propios usuarios en el ataque. Algunos ejemplos relevantes de las consecuencias de este tipo de ataque son:
 - Ser parte de una BOTnet (red de zombies): el sistema atacado pasa a ser parte de una red de ordenadores controlados remotamente por el atacante, el cual los programa para realizar actividades ilícitas (envío de correo basura a millones de destinatarios, etc.)
 - Ser víctima del ataque denominado “ransomware”, o secuestro digital: el atacante cifra determinados ficheros en los sistemas atacados exigiendo un rescate económico para poder descifrar dichos ficheros.
 - APTs (Advanced Persistent Threats, o Amenazas Persistentes y Avanzadas): una combinación de técnicas de ataque, que pueden incluir uso de distintos tipos de vulnerabilidades con técnicas de ingeniería social, diseñadas específicamente para un ataque a una determinada organización. El hecho de no usar técnicas de ataque genéricas, sino particularizadas para una organización y sus usuarios, hace que esta técnica tenga un alto grado de éxito y sea una de las amenazas más peligrosas actualmente para las organizaciones.



- Ataques a Infraestructuras Críticas: cuando la motivación es política, militar o terrorista, los atacantes pueden intentar buscar vulnerabilidades en sistemas de control de dichas infraestructuras con graves consecuencias.

Las amenazas de seguridad a una infraestructura de redes y servicios de telecomunicación pueden clasificarse de la siguiente forma, dependiendo del objetivo principal del ataque:

- ▶ Amenazas Humanas: ataques dirigidos al usuario final de los sistemas, intentando su colaboración involuntaria en el ataque. Para ello, necesitan engañar al usuario para que ejecute un cierto programa, o revele cierta información (ataques de ingeniería social). Estos ataques, sobre todo cuando están hechos a la medida del usuario objetivo, pueden ser muy complicados de detectar y bloquear técnicamente, por lo que las medidas de seguridad deben pasar por campañas formativas y de concienciación en la seguridad para todo tipo de usuarios de sistemas informáticos
- ▶ Amenazas Tecnológicas: ataques dirigidos a explotar una vulnerabilidad de los programas o de sus configuraciones. En caso de vulnerabilidades de día 0, estos ataques pueden ser muy complicados de detectar y



bloquear. En caso de vulnerabilidades conocidas, es necesario aplicar cuanto antes los parches proporcionados por los fabricantes para solucionar dicha vulnerabilidad.

Estrategia de seguridad ante las amenazas

La estrategia de seguridad de una organización ante este tipo de amenazas debe venir de una actuación en dos frentes: una *estrategia organizativa de seguridad*, que involucre a los órganos de gestión y dirección de la organización, para definir los objetivos de seguridad, así como los procesos y procedimientos necesarios para la implementación de dicha estrategia, y una *estrategia tecnológica de seguridad*, que debe ser consecuencia de la primera, y que incluirá un subconjunto de las distintas tecnologías de seguridad existentes en el mercado actualmente adecuadas para los riesgos específicos de dicha organización.

Estrategia organizativa

Las actuaciones en el área de ciberseguridad de una organización no deben ser definidas por los técnicos, a nivel tecnológico, sino que deben emanar de una estrategia de alto nivel realizada desde la dirección de la organización. Esta estrategia se debe plasmar en el diseño y

ejecución de un *Plan Director de la Seguridad*, que permita definir y priorizar un conjunto de proyectos de ciberseguridad para reducir los riesgos de seguridad a los que está expuesta la organización. Para ello, usualmente este Plan Director de Seguridad debe ser abordado en diversas etapas:

- ▶ Conocer la situación actual de la organización, definiendo claramente el ámbito de actuación, los actores y responsables involucrados y desarrollar una valoración de la situación actual de la organización, con una auditoría que verifique la existencia y eficacia de los controles. Para realizar esta valoración son de gran utilidad los controles generales establecidos en la norma ISO 27002:2013, que recoge un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.
- ▶ Definir los objetivos de seguridad a los que se quieren llegar, teniendo en cuenta la estrategia corporativa de la organización, para llegar a definir la Política de Seguridad de la organización.
- ▶ Realizar un Análisis de Riesgos que establezca los niveles de riesgo asumibles por la organización, y proponer un conjunto de controles y salvaguardas que permita obtener los niveles de seguridad objetivos definidos en la política de seguridad.
- ▶ Definición de Proyectos e Iniciativas en distintos ámbitos para implantar los controles y salvaguardas anteriores. Estos proyectos serán clasificados y priorizados, incluyendo una propuesta de planificación temporal, esfuerzo y coste necesario para su ejecución. Estos proyectos deberán incluir el diseño y puesta en marcha de un Sistema de Gestión de la Seguridad de la Información (SGSI), que gestione dichos controles y salvaguardas y permita su verificación.
- ▶ Aprobación del Plan Director de Seguridad, por parte de la Dirección de la Organización e Implantación del Plan Director de Seguridad, con la ejecución de los distintos proyectos según la planificación aprobada.

Adicionalmente, la organización deberá diseñar e implantar un *Plan de Continuidad de Negocio* que permita a las organizaciones estar preparadas para prevenir, protegerse y reaccionar ante incidentes de seguridad que pueden afectarles con impacto en el negocio de la organización. Por ello, este plan debe contener un conjunto de tareas que le permita a la organización recuperarse tras un incidente en un plazo adecuado de tiempo, que no comprometa la continuidad de su negocio.



Estrategia tecnológica

Como parte de los proyectos diseñados en el Plan Director de Seguridad, será necesario la implantación de controles técnicos y la gestión de los riesgos de seguridad, que necesitarán la implantación de herramientas específicas de seguridad. Para ello, los fabricantes de seguridad proporcionan múltiples soluciones actualmente, que pueden ser agrupadas de la siguiente forma:

- ▶ Servicios de Control de Acceso: estas herramientas permiten implantar y gestionar la identificación de las personas y los recursos involucrados en los sistemas de información. Para ello, la tecnología actual ofrece múltiples sistemas de autenticación (claves simétricas, claves asimétricas e infraestructura de clave pública asociada, tarjetas, sistemas biométricos, etc.), sistemas de gestión de autenticación que permita soluciones de autenticación centralizada (Single Sign On) o federada, sistemas NAC (Control de Acceso a Red), Redes Privadas Virtuales, etc. En estos servicios, también se incluyen los servicios que permiten gestionar las autorizaciones asociadas a cada persona o recurso identificado.
- ▶ Servicios de Defensa Perimetral, que permita una protección global de un conjunto de sistemas, actuando antes de que los ataques lleguen a sus objetivos. Aquí se pueden encontrar las distintas familias de cortafuegos (cortafuegos de red, de aplicación, de Web, etc.), así como sistemas de detección y prevención de intrusiones (IDS/IPS), sistemas de análisis e inspección de contenidos para la detección de malware, etc.
- ▶ Servicios de Protección de la Información, que permita gestionar los distintos requisitos de privacidad de la información gestionada en una organización (tanto almacenada como en tránsito), de acuerdo a las políticas y normativas aplicables. En esta área el mercado ofrece soluciones de cifrado y firmado de la información, protección ante fuga de información (Sistemas DLP, Data Leak Protection), gestión de derechos digitales, seguridad en protocolos de red, etc.

Esta estrategia tecnológica de la propia organización debe complementarse con las garantías de seguridad necesarias en los servicios de terceros que la organización tiene contratados. El ejemplo más claro es el de la Computación en la Nube, en el que la organización debe definir claramente los requisitos de seguridad aplicable a la información y servicios usados en la nube, así como los acuerdos necesarios para garantizar el cumplimiento de dichos objetivos.

Evolución futura

Los últimos años han supuesto un periodo de madurez en el campo de la seguridad en Internet. Los fabricantes de productos han tomado conciencia del problema y son cada vez más exigentes en cuanto a la calidad del *software*, y en el mantenimiento de sus productos con actualizaciones que solucionen problemas de seguridad. Por otra parte, se ha extendido la inclusión de tecnologías de seguridad en las organizaciones y en los sistemas individuales que ha permitido que disminuya el número de vulnerabilidades importantes en Internet.

Sin embargo, esto ha hecho a su vez que los atacantes hayan modificado su estrategia y actualmente hayan derivado el objetivo del ataque desde los sistemas informáticos hacia los usuarios. Los ataques de ingeniería social se han multiplicado en los últimos años y muchos de las grandes incidencias recientes son consecuencia de un engaño a los usuarios para que ejecuten cierto código, o se conecten a ciertas páginas, etc. Por ello, es muy importante actualmente los aspectos de *formación y concienciación* a distintos niveles: capacitación de expertos, formación de empleados en organizaciones y administraciones públicas y concienciación de ciudadanos.

Desde un punto de vista tecnológico, la evolución de los ataques va tomando forma en tres frentes: ataques a dispositivos móviles, con un grado de madurez todavía insuficiente en su protección, ataques a la denominada Internet de las Cosas, con una gran variedad de dispositivos muchas veces desatendidos, con la problemática de gestión de seguridad que puede suponer, y los ya comentados ataques a sistemas de control de Infraestructuras Críticas. ☺

Cybersecurity: New Threats, New Strategies

In this article, Professor Villagra provides an historical overview of the evolution of the concept of cybersecurity, from the outset of

the Internet up until today's advent of the mature field of Internet security. In it, he analyzes the evolution of the threats

involved and the alternative approaches to putting effective security strategies into place.