DEFENSA EN PROFUNDIDAD PARA LA PROTECCION CONTRA LAS AMENAZAS PERSISTENTES AVANZADAS

Cantor Ospina, Nohora Milena

***Abstract*—In recent years there has been a growing interest in attackers on the knowledge of new technologies and emerging trends to be able to use them as a link to users and make them part of their deception strategies; In this way, new ways of entering within the private domains of the organizations are found and the technical security concept of Advanced Persistent Threat (APT).**

It is intended to present the different advanced threat detection systems that currently exist in the market, and how they have become a further barrier to security in organizations and inclusion within defense-in-depth schemes.

***Index Terms*—Defensa en profundidad, amenazas persistentes avanzadas, atacante, amenaza, seguridad física, seguridad lógica.**

I. INTRODUCCION

En los últimos años se ha evidenciado un mayor interés del uso de tecnologías nuevas y emergentes por parte de atacantes informáticos, teniendo como base a los usuarios finales para hacerlos parte de sus estrategias de engaño; basados en estas tecnologías, los atacantes encuentran nuevas formas de incursionar en los dominios privados de las organizaciones. Estos comportamientos abren paso al concepto técnico en seguridad de "Amenazas Persistentes Avanzadas. (Advanced Persistent Threat) conocido como APT.

Estas amenazas llegan a convertirse en ciberataques de crecimiento exponencial que las organizaciones deben afrontar en sus labores diarias. Los atacantes informáticos por medio de estrategias, logran tomar por sorpresa a los empleados, incursionan en los sistemas de la compañía y consiguen comprometer información, llegando a incurrir en costos financieros, pérdida de información y hasta denegación de servicios, lo que obliga a las entidades a protegerse frente a este tipo de vulnerabilidades.

Con base en esto, los atacantes hacen reconocimiento continuo de los movimientos de los empleados, utilizando como insumos, por ejemplo, información publicada en redes sociales en las que se describen gustos, tendencias y motivaciones; y logran aplicar estrategias de ingeniería social, creando perfiles de comportamientos que logran dejar al descubierto formas de ingreso a su información confidencial o a infraestructuras tecnológicas con las cuales está interactuando.

Teniendo en cuenta que estas amenazas pueden esperar pacientemente al interior de un sistema de información, y que el nuevo escenario de estos ataques muestra que se mantiene un constante monitoreo de los sistemas, los intrusos reconocen en las personas el eslabón más débil de la cadena, encontrando la forma de superar las barreras tecnológicas que las empresas puedan tener en su perímetro. Por esta razón se hace necesario incluir y evaluar el concepto de Defensa en Profundidad (Defense in Depth) como estrategia en la implementación de controles para la protección de los datos en sus diferentes capas, minimizando así el ingreso de estas amenazas en la organización.

A continuación, se presentará una descripción del modelo de defensa en profundidad, del entorno actual de las APT's y su recorrido con el paso del tiempo, partiendo desde la definición de seguridad informática hasta los diferentes tipos de detección para esta clase de amenazas y como se puede convertir en una barrera adicional dentro del concepto de defensa en profundidad.

II. SEGURIDAD INFORMÁTICA

La Seguridad Informática es el conjunto de buenas prácticas implementadas, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información, podemos clasificarla de dos formas.

A. Seguridad Física

Cuando se habla de seguridad física en el ámbito de la seguridad informática, hacemos referencia a la custodia del hardware y todos los componentes físicos de un sistema informático, los cuales deben estar resguardados y protegidos de la manipulación de personal externo o no autorizado y lejos del alcance de los delincuentes o cualquier acto delictivo.

B. Seguridad Lógica

La seguridad lógica hace énfasis a los controles de software que se aplican a los sistemas informáticos, estos son los encargados de garantizar que solo las personas indicadas tengan acceso a los datos almacenados en estos sistemas.

III. Amenazas Persistentes Avanzadas

Las Amenazas Persistentes Avanzadas o APT's (Advanced Persistent Threats) son ataques dirigidos a infraestructuras informáticas; con el fin de obtener información para beneficio económico, financiero e incluso para beneficio personal o industrial.[1] Se caracterizan por estar "enmascaradas" en un programa o en un documento que contiene información de interés orientado a un público especifico, por perdurar en el tiempo sin ser detectadas infectando la mayor cantidad de dispositivos en la red y por camuflarse como tráfico legitimo para el usuario y aprovechar las vulnerabilidades desconocidas en el sistema infectado; logrando de esta manera ser más efectivo a la hora de realizar el ataque.

IV. Proceso de Ataque de una APT

El proceso de ataque de estas amenazas se basa en técnicas que utilizan software malicioso para lograr explotar vulnerabilidades e involucran actividades de ingeniería social para obtener información digital, verbal y/o física de un sistema. Este proceso permite enmascarar ataques reales sobre tráfico legítimo para lograr inyectarlos a la red y de esta manera no ser descubiertos. Este proceso de ataque se compone de 3 etapas: El estudio o preparación del ataque, el lanzamiento o propagación del ataque y la extracción y/o acceso a los recursos de la información.

A. Estudio o preparación del ataque

El atacante realiza un estudio a fondo de la víctima utilizando un reconocimiento continuo de sus intereses tomando como insumos, por ejemplo, información publicada en redes sociales en las que se describen gustos, tendencias y motivaciones; y logran aplicar estrategias de ingeniería social, creando perfiles de comportamientos que logran dejar al descubierto formas de ingreso a su información confidencial o a infraestructuras tecnológicas con las cuales está interactuando.

B. Lanzamiento o propagación del ataque

El atacante envía un mensaje con información de interés a la persona que se le realizó el proceso de ingeniería social; la persona ingresa al mensaje enviado y propaga el ataque a través de la red en la que se encuentra. Tras la infección, el ataque se desplaza logrando avanzar progresivamente a una instancia más alta, llegando al lugar en que se encuentra la información más valiosa de la organización. Este ataque también se suele ejecutar desde dispositivos infectados que posteriormente son ingresados y conectados en cualquier equipo de cómputo de la compañía como lo sería por ejemplo una USB infectada.

C. Acceso a los recursos y/o extracción de la información

El atacante planea la ejecución de la tercera etapa dependiendo del tiempo que él piensa puede permanecer en la red sin ser descubierto. Esta etapa consiste en extraer la mayor cantidad de información en el menor tiempo posible.

Valiéndose de un hosting externo inicia la transferencia de archivos en carpetas comprimidas a través de un servicio previamente instalado y configurado. Este ataque también puede ser ejecutado por el atacante en caso de ser descubierto logrando propagarse en la mayor cantidad de dispositivos en la red.

V. Método de Infección y Propagación de APT

Existen diferentes métodos para la infección y propagación de APT's. Estos métodos son categorizados en causas internas y causas externas:

A. Causas internas

En las causas internas se encuentran vulnerabilidades que afrontan frecuentemente la organizaciones, tales como desactualización de los sistemas, falta de aseguramiento (hardening) físico, ausencia de dispositivos de seguridad, infraestructura tecnológica obsoleta, ingreso de dispositivos personales que permiten la propagación de amenazas y la materialización de vulnerabilidades del día cero, de las cuales los atacantes sacan el mayor provecho, ya que no existe una actualización inmediata que pueda corregir esta vulnerabilidad, y los atacantes pueden tomar control del sistema hasta que la falla sea corregida.

Otra de las causas internas y de mayor cuidado son los recursos humanos. El desconocimiento del manejo de sistemas informáticos permite, en la mayoría de los casos, la ejecución de malware que pueden infectar un sistema de información, sin que la persona tenga alguna intención de propagar el ataque.

B. Causas externas.

Las causas externas logran persuadir a las personas, permitiendo la ejecución de manera involuntaria, de comandos, programas o incluso tareas programadas para lograr la infección del sistema; la causa más común que los atacantes están usando es el phishing, técnica de ingeniería social que se ejecuta con la intención de suplantar un sistema informático, pagina web o correo electrónico y tiene como fin obtener información de usuarios y contraseñas.[2] En el caso de las APT's el tipo de phishing usado es el dirigido, con el cual se pretende obtener la información directamente de los involucrados en los procesos del negocio como son los directivos, gerentes, directores o coordinadores.

Otra de las causas externas que las organizaciones afrontan es el uso de dispositivos personales infectados que al ser conectados en la red, propagan la amenaza a los demás dispositivos. Esta técnica suele ser la más efectiva cuando al interior de la compañía no se cuenta con ninguna clase de control de seguridad. La ausencia de controles en la organización como los dispositivos de seguridad firewall, IPS, antivirus entre otros hacen que la red se encuentre susceptible a estos tipos de ataques.

[1] VILLALÓN, Antonio. Amenazas Persistentes Avanzadas. Annapolis Exchange Parkway.: NAU Libres. ISBN 978-84-16926-09-1.

[2] GLENY, Misha. El lado oscuro de la red. La nueva mafia del ciberespacio. Traducido por David Paradela López. vol. 216. Barcelona: Ediciones Destino, 2012. 15 p. ISBN 978-84-233-4584-7.

VI. Defensa en Profundidad

El

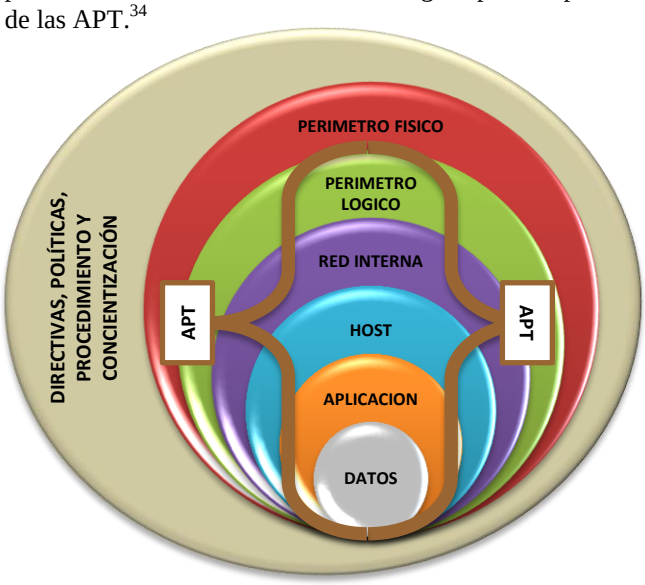
concepto de Defensa en Profundidad se establece como la protección con barreras independientes de un sistema informático. El concepto de barrera se encuentra ligado al componente de protección (limitación, separación, etc.) y para nuestro entorno IT (Tecnologías de información) se aplica como un modelo para garantizar niveles de seguridad aceptables, aplicando barreras mínimas de protección a la infraestructura de tecnología, la cual alberga uno de los activos más valiosos para las organizaciones: la información.

Un sistema informático puede ser representado por una serie de capas en el que la información ocupa el último nivel y el cual precede de algunas características físicas, contenedores perimetrales, redes, servidores y aplicaciones.

Con esto cada capa del sistema representa una barrera que debe sobrepasar un atacante para lograr acceder a los datos importantes de la organización, de forma que, si se ve comprometida alguna barrera, se cuenta con defensas adicionales que contienen la amenaza y minimizan las probabilidades de materialización de algún tipo de riesgo.

Existen modelos de defensa en profundidad sobre sistemas informáticos definidos por autores o firmas como Microsoft, Esset, entre otros, que identifican para cada capa un grado adecuado de defensa, y su propósito principal se centra en reducir al máximo la probabilidad de que un atacante alcance su objetivo. Para cada nivel existen varias formas de protección como herramientas, tecnologías, directivas, etc

A continuación se describe un modelo de defensa en profundidad sobre un sistema tecnológico para la protección de las APT.[3][4]



DIRECTIVAS, POLÍTICAS, PROCEDIMIENTO Y CONCIENTIZACIÓN

- Políticas de seguridad de la información
- Política General
- Programas de aprendizaje continuo de seguridad
- Procedimientos, estándares y buenas practicas

PERIMETRO FISICO

- Circuitos Cerrados de Televisión CCTV
- Controles de acceso físico
- Alarmas
- Vigilancia
- Protección contra desastres naturales

APT

- Amenazas persistentes avanzadas - Solución Transversal para las capas, (Perímetro Lógico, Red Interna, Host, Aplicación, Datos)

PERIMETRO LOGICO

- Sistemas de detección/ prevención de intrusos (IPS /IDS)
- Firewall de nueva generación (NGWF)
- Conexiones Virtuales (VPN)
- Prevención amenazas (APT)

RED INTERNA

- Segmentación de red - VLAN
- Listas de Control de Acceso (ACL)
- Seguridad en puertos
- Control de acceso en la red (NAC)
- Protocolos de Cifrados
- NIP

HOST

- Aplicación Directivas
- Limitación Servicios y/o App
- Control de Accesos
- Estándares de Hardening
- Herramientas de Administración (Parches, actualizaciones etc.)
- Antivirus // HIPS

APLICACION

- Técnicas de Programación Segura
- Revisión de Código
- Controles de acceso
- Protocolos de Cifrado
- Firewall de Aplicaciones Web (WAF)

DATOS

- DLP - (Data Loss Prevention)
- ACL sobre archivos
- Sanitación de Datos
- Digital Rights Management DRM

Fig. 1. Modelo de Defensa en Seguridad.

[3] Modelo de Defensa en Profundidad - Microsoft [en línea]. Colombia: Portafolio Blogs mar. 2016. Disponible en Internet: <https://es.scribd.com/presentation/57403910/Modelo-de-Defensa-enProfundidad-Microsoft>

[4] Defensa de Seguridad - Sebastián Bortnik – Welivesecurity [en línea] Articulo may. 2010. Disponible en Internet: <https://www.welivesecurity.com/la-es/2010/05/24/defensa-en-profundidad/>

A. Capa de directivas, políticas, procedimientos y concientización:

Debido a que un atacante informático reconoce en las personas el eslabón más débil para superar las barreras tecnológicas que encuentre en un perímetro, es necesario limitar el acceso a los sistemas, y garantizar e informar un debido uso de los derechos y deberes que se concedan a los usuarios que acceden a estos sistemas. Es necesario establecer:

- Políticas de seguridad de la información y buenas practicas definidas en una política general de la compañía.
- Programas de aprendizaje continuo de seguridad de la información para los usuarios.

B. Capa de seguridad física:

Se deben implementar controles de seguridad física adecuados para garantizar que ningún intruso intente sabotear o causar algún daño físico al sistema, particularmente en áreas sensibles como centros de cómputos, datacenters, e incluso los edificios en donde se encuentra el personal. La seguridad física se debe considerar como un elemento transversal en la implementación de seguridad, apoyando la protección en elementos como:

- Circuitos Cerrados de Televisión CCTV.
- Controles de acceso físico (Sistemas Biométricos, Tarjetas inteligentes).
- Alarmas.
- Vigilancia (Guardias de Seguridad).
- Protecciones contra desastres naturales.

C. Capa Perimetral

Esta capa se convierte en la primera línea de defensa para proteger el perímetro de la red de ataques externos. Se requiere que se evalué cada control y dispositivo dentro de esta capa, con el fin de poder identificar el tráfico legítimo, poder permitirlo, y realizar el bloqueo para el tráfico desconocido; se necesitara uno o más dispositivos de seguridad para contener y minimizar los ataques externos.

Debido a la cantidad de ataques que se generan en esta capa se incorporan cada vez más características y dispositivos para su protección. En esta capa se identifican dispositivos como:

- IPS (Intrusion Network System) – Sistema de detección de intrusos usado para la prevención y monitoreo de actividades sospechosas sobre la red en tiempo real.
- NGFW (Next Generation Firewall) – Firewall de nueva generación que incluye funcionalidades de filtrado de contenido, detección de intrusión (IPS/IDS), VPN (Virtual Private Network),
- Antivirus.
- VPN (Virtual Point Network), - Sistema usado para asegurar las conexiones con terceros o remotas.
- APT (Advanced Persistent Threat) – Sistema utilizado para detección y prevención de amenazas persistentes avanzadas.

D. Capa Red Interna

En la estructura de la organización el tráfico interno se segmenta por medio de VLAN's, de manera que solo los equipos identificados en una misma VLAN puedan comunicarse. Algunos ejemplos de tecnologías en esta capa son:

- VLAN - Segmentación de red.
- ACL – Aseguramiento de la red restringiendo que dispositivo puede comunicarse con otro dispositivo (incluyendo las máquinas de una misma vlan).
- Seguridad lógica en los puertos físicos – Uso de tecnologías como Port-security CISCO.
- NAC – Aseguramiento de los usuarios finales.
- Uso de algoritmos de cifrado en las comunicaciones como un mecanismo que permita la comunicación segura por un canal cifrado (IPSEC, SSL, AES, DES, SHA etc.).
- NIPS – Sistema de detección de intrusos basados en red – Detección de ataques en los segmentos de red.

E. Capa de Host:

Es necesario reforzar los controles dirigidos a los servidores, equipos finales y/o clientes, por lo que se hace necesario evaluar cada dispositivo de este entorno y aplicar una serie de controles como:

- Directivas por funciones ya sea por su clasificación y/o tipo de datos. Ej. 1. Servidor Web-Uso público-Información pública. 2. Servidor Base de Datos-Uso confidencial-Información restringida.
- Limitación de aplicaciones y servicios.
- Controles de acceso.
- Aplicación de Hardening.
- Herramientas de administración (Revisión, actualizaciones, parches etc.).
- Métodos seguros de autenticación.
- Antivirus.
- HIPS – Sistema de detección de intrusos basados en host– Detección de ataques a los dispositivos finales.

F. Capa Aplicación

Es esencial reforzar los controles dirigidos a las aplicaciones, como una capa adicional de defensa. La mayoría de aplicaciones utilizan subsistemas para su funcionamiento (entorno), estos pueden ser alterados por un atacante afectando cualquier componente de este entorno afectando las aplicaciones. Se debe tomar medidas de protección como:

- Programación segura de las aplicaciones (Eliminación de configuraciones por defecto).
- Control de acceso a nivel de la aplicación.
- Revisión de código.
- Protocolos de cifrado.
- WAF (Web Firewall Application) – Firewall dedicado a la detección de comportamientos anómalos sobre las aplicaciones.

- Aseguramiento sobre el entorno de las aplicaciones.

G. Capa Datos

Por último, se encuentra la capa en la que se ubica el activo más valioso para las organizaciones, la Información; garantizar los pilares de seguridad tales como confidencialidad, disponibilidad e integridad es fundamental y debe evitarse que estos puedan ser extraídos y se pierda el control de los mismos por personas no autorizadas. Se deben realizar controles sobre los datos utilizando procedimientos como:

- Controles de Acceso.
- Protocolos de Cifrado.
- DLP - (Data Loss Prevention).
- Sistemas de cifrado.
- ACL sobre archivos.

H. Detección de APT

Cuando es realizado un ataque informático y logra ser exitoso, las compañías pueden tardarse días e incluso meses en detectar que fueron víctimas de un ataque. Para una óptima defensa contra un ataque de APT es necesario contar con un equipo interdisciplinario con profesionales en diferentes áreas de tecnologías de la información, e incluso monitorear permanentemente la red, para proteger 24horas – 7 días a la semana, la compañía de dichos ataques.

Para facilitar la defensa, algunos fabricantes líderes en tecnología han desarrollado poderosos sistemas de monitorización en tiempo real, que abarcan varias capas del modelo de defensa. contribuyendo al análisis y detección de amenazas, antes de comprometer la seguridad de la información de la compañía.

1) Sistema de detección de APTs FireEye

Es considerado como uno de los líderes en la lucha contra las nuevas amenazas a la seguridad informática, como son los ataques de "día cero" y APTs. Su plataforma complementa la seguridad perimetral existente, basada en firewalls y sistemas IPS. Sus sistemas proporcionan un eficaz defensa sobre todas las fases del ciclo de vida de la amenaza, gracias a su tecnología patentada que permite ejecutar las posibles amenazas en tiempo real dentro de un ambiente virtual.

2) Sistema de detección de APTs TrendMicro.

Este fabricante de software y hardware también presenta su solución frente a los ataques de APTs por medio de su Trend Micro Custom Defense, el cual permite detectar, analizar y bloquear estos ataques, basado en su repositorio de información sobre amenazas mundiales y sus herramientas que brindan una acción rápida y oportuna sobre este tipo de amenazas.

VII. CONCLUSIONES

Hoy en día no solo los sistemas de información son escalables, las amenazas también lo son. Esto obliga a las compañías, protegerse frente este tipo de amenazas evaluando de manera detallada la implementación de un modelo de defensa contra ataques APT's para combatir de una manera rápida, eficaz y oportuna este tipo de amenazas.

La defensa en profundidad aumenta significativamente la seguridad del sistema. Cada capa del modelo de defensa en profundidad es independiente, pero es posible agrupar varias de estas capas mediante un dispositivo de control de APT. Utilizar un dispositivo por cada capa conlleva un costo adicional; por tanto, es necesario evaluar si la importancia de la información a proteger justifica la implementación de una, dos, o las capas de seguridad que sean necesarias, o por el contrario si la implementación de un único dispositivo de control APT suple las necesidades de la organización.

El modelo de defensa en profundad aumenta las probabilidades de detectar rápida y eficazmente un intruso, y disminuye las probabilidades de que su ataque tenga éxito. Es de gran importancia que el diseño y la implementación de dispositivos de control de APT en cada capa, permita que cada capa superior sea más rigurosa en la revisión del tráfico que se está analizando.

Las organizaciones deben implementar esquemas de capacitación a su personal, con el fin de dar a conocer las nuevas metodologías que están utilizando los atacantes para acceder a los sistemas de información. Metodologías como la Ingeniería Social, en donde se aprovecha la vulnerabilidad de la persona para extraer información, y obligar indirectamente a la persona a ejecutar acciones que permitan el acceso de estos atacantes a los sistemas de información.

REFERENCES

[1] VILLALÓN, Antonio. Amenazas Persistentes Avanzadas. Annapolis Exchange Parkway.: NAU Libres. ISBN 978-84-16926-09-1.

[2] GLENY, Misha. El lado oscuro de la red. La nueva mafia del ciberespacio. Traducido por David Paradela López. vol. 216. Barcelona: Ediciones Destino, 2012. 15 p. ISBN 978-84-233-4584-7.

[3] DÍAZ, José Antonio y SALCEDO, Juan Diego, Sistema de Prevención de Intrusos para mejorar la seguridad de los servidores de la Universidad Nacional de Trujillo. Plan de Proyecto de Trabajo de Graduación. Perú.: Universidad Nacional De Trujillo. Facultad De Ciencias Físicas Y Matemáticas

[4] PIPER, Steaven.Definitive Guide para la Protección contra amenazas de próxima generación. s.I : CyberEdge Group, LLC. ISBN 978-0-98882331-0.

[5] MILLER, Ruseell. Amenazas persistentes avanzadas: la defensa desde adentro hacia afuera. CA Technologies, 2012. Disponible en Internet: < http://www.arcserve.com/~/media/Files/whitepapers/latam/CS2548_ad v anced_persistent_threats_wp_0712_las.pdf>

[6] Understanding the advanced persistent threat. Information Security Magazine. Julio, 2010, vol. 22, no. 6.

[7] HOLGUÍN, José Miguel, MORENO, Maite y MERINO, Borja, Deteccion de APTs. S2Grupo, 2013. Disponible en Internet: <https://s2grupo.es/wp-content/uploads/2017/01/deteccion_apt.pdf> [8] Qué son las amenazas persistentes avanzadas (APTs) [en línea]. España: Instituto Nacional de Tecnologías de la Comunicación. Disponible en Internet: <www.egov.ufsc.br/portal/sites/default/files/cdn_apts.pdf>

[9] Amenazas persistentes avanzadas ¿Está preparado su negocio? [en línea]. Colombia: Portafolio Blogs mar. 2016. Disponible en Internet: <http://blogs.portafolio.co/tecnologia-personal/amenazaspersistentesavanzadas/>

[10] Defense in the depth, SANS Insititute Information Security Reading Room, Todd McGuiness. Noviembre, 2011. Disponible en Internet: <https://www.sans.org/reading-room/whitepapers/basics/defense-indepth-525>

[11] Modelo de Defensa en Profundidad – Mónica Fernández - Microsoft [en línea]. Colombia: Portafolio Blogs mar. 2016. Disponible en Internet: < https://es.scribd.com/presentation/57403910/Modelo-de-Defensa-enProfundidad-Microsoft>

[12] Defensa de Seguridad - Sebastián Bortnik – Welivesecurity [en línea] Articulo may. 2010. Disponible en Internet < https://www.welivesecurity.com/la-es/2010/05/24/defensa-enprofundidad/>

[13] Defensa en profundidad aplicado a un entorno empresarial – GUIJARRO, Alfonso A, YEPEZ, Jessica M, PERALTA, Tania J, ORTIZ, MirellaC, Vol. 39 (Nº 42), 2018 Pág. 19 [en línea]. Disponible en Internet < http://www.revistaespacios.com/a18v39n42/a18v39n42p19.pdf

[14] Gestión estratégica de seguridad en la empresa, ANETCOM. 2008 Disponible en Internet: <https://www.csirtcv.gva.es/sites/all/files/downloads/Seguridad_empres a.pdf>

[15] Modelo de Seguridad en Profundidad, GuarNET, 2011. Disponible en Internet:<http://guardnet.wordpress.com/2011/06/08/modelo-deseguridad-en-profundidad/>