CTN

CIBERSEGURIDAD

BIG DAT & I.A.

PARA DETECCIÓN DE ANOMALÍAS

INFORME DE VIGILANCIA TECNOLÓGICA

2020

Unión Europea

Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

RIS3 MUR

info REGIÓN DE MURCIA

Este informe ha sido elaborado por la Asociación Empresarial de Investigación Centro Tecnológico Naval y del Mar gracias al Convenio suscrito con el Instituto de Fomento de la Región de Murcia con el apoyo del fondo FEDER.

Autores: Pablo Ruiz, Rubén Correoso, Pedro Molina, Paula Gómez y Mª Ángeles García Albaladejo

Más info: www.ctnaval.com

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

Índice

Índice de imágenes

1. Introducción

Este informe, elaborado por el equipo del Centro Tecnológico Naval y del Mar, tiene como finalidad ofrecer al tejido empresarial una mejora en el conocimiento del entorno, que permita detectar tendencias y desarrollar estrategias adecuadas basadas en niveles superiores de certidumbre a través de la captación y divulgación de información y conocimiento de importancia estratégica en los ámbitos social, tecnológico y económico, que incidan en la detección de nuevas oportunidades de desarrollo regional.

Los contenidos de este informe están estrechamente relacionados con el desarrollo del proyecto *Uso de técnicas avanzadas de Big Data e Inteligencia Artificial para la detección de anomalías en el ámbito de la ciberseguridad* financiado por el Instituto de Fomento de la Región de Murcia.

Para la realización de este informe se han aplicado técnicas de Vigilancia Tecnológica, una herramienta al servicio de las empresas y organizaciones que permite detectar oportunidades y amenazas aportándoles ventajas competitivas y fundamentos para la toma de decisiones estratégicas mediante la selección y análisis de información de diversos tipos (científica, tecnológica, comercial, de mercado, social…).

Para ello se parte de una introducción metodológica sobre las técnicas y fases de la Vigilancia Tecnológica que se han aplicado para el desarrollo del informe. Seguidamente se realiza un análisis del estado de la técnica, noticias, proyectos y literatura científica.

Por último, se incluyen las fuentes que se han manejado para la realización de este informe.

2. Metodología

La vigilancia tecnológica se entiende como una "forma organizada, selectiva y permanente de captar información del exterior sobre tecnología, analizarla y convertirla en conocimiento para tomar decisiones con menor riesgo y poder anticiparse a los cambios". (AENOR, 2011) Su finalidad última es generar ventajas competitivas para la empresa ya que le proporciona datos para:

Ilustración 1. Finalidad de la Vigilancia Tecnológica

Para el desarrollo de la Vigilancia Tecnológica el primer paso el plantear los aspectos básicos (Degoul, 1992):
¿Cuál es el objeto de la vigilancia? ¿Qué debemos vigilar? ¿Qué información buscar? ¿Dónde localizarla?

Cuando el objetivo de la VT está claramente delimitado, se procede a planificar la estrategia de búsqueda. Para el despliegue de esta fase conviene tener en cuenta que la información puede presentarse de dos formas: estructurada y no estructurada. La primera es propia de las bases de datos, conjuntos de datos homogéneos, ordenados de una forma determinada, que se presenta en forma legible por ordenador (Escorsa, 2001). Su unidad es el registro –o ficha de un artículo científico o una patente- que presenta la información ordenada en campos: autor, título, fecha de publicación, titular de la patente, inventores, etc. En cambio, la información no estructurada se presenta en textos sin un formato determinado (noticias de periódicos, sitios web, blogs, correos electrónicos) cuyo tratamiento requerirá de nuevas herramientas capaces de "leer" y analizar estos textos. Estas herramientas son útiles también para analizar la información de textos completos de artículos

científicos o de patentes. Hoy se considera que el texto es la mayor fuente de información y conocimiento para las empresas. (Escorsa, Pere, Pilar Lázaro Martínez, Círculo de Innovación en Biotecnología, 2007).

Tras la selección de las palabras clave se automatiza la búsqueda en función de las diferentes tipologías de fuentes a utilizar, se lanza la misma y se filtran los resultados en términos de pertinencia, fiabilidad, relevancia, calidad y capacidad de contraste (AENOR, 2011).

Una vez comprobada la calidad de la información, los métodos de análisis han de garantizar su valor para la explotación de los mismos (F. Palop, 1995). El objetivo del análisis es transformar la información en bruto recogida en un producto con alto valor añadido. A partir de aquí, la aportación de los expertos es crítica para crear información avanzada, para generar conocimiento. Pasamos de una masa ingente de información en distintos formatos y lugares a una etapa en la que se captura la información más relevante, se organiza, indexa, almacena, filtra y, finalmente, con la opinión del experto que aporta en este punto del proceso un máximo valor añadido (CETISME, 2003).

A continuación, se incluye un esquema con las distintas fases de la metodología empleada durante la generación de este informe.

Ilustración 2. Fases de la Vigilancia Tecnológica

3. Estado del arte

A continuación, se describe el estado del arte de las principales vulnerabilidades en ciberseguridad y las posibles soluciones que se han desarrollado hasta ahora, diferenciándolas en tres grupos principales:

1. Nivel de red
2. Nivel de servidor
3. Nivel de aplicación

3.2 Ciberseguridad a nivel de Red

Man-in-the-middle (Secuestro de sesión): en un ataque Man-in-the-middle[1], el atacante retransmite y altera la comunicación entre dos partes que creen que se están comunicando directamente entre sí. Con el secuestro de sesión, el pirata informático aprovecha las vulnerabilidades de los sistemas para obtener los mismos derechos de acceso que los clientes objetivo (por ejemplo, cookies de autenticación). Existen múltiples ataques basados en Man-in-the-middle a continuación se explican tres de los ataques más comunes:

1. Ataques basados en servidores DHCP: un hacker que coloca su propio ordenador (o uno que esté bajo su control) en una red de área local (LAN) a modo de servidor DHCP. Con ello, los hackers tienen la posibilidad de controlar la adjudicación de direcciones IP locales mediante el servidor DHCP simulado, de registrar las puertas de acceso que se deseen y el servidor DNS en los ordenadores a los que se ha engañado y, por lo tanto, de desviar el tráfico de datos saliente a cualquier ordenador para interceptar y manipular contenidos.

2. Envenenamiento ARP: la asignación de direcciones MAC a IP locales se guarda en forma de tabla en el caché ARP del ordenador que solicita la información. Es aquí donde actúa el llamado envenenamiento de cache ARP. El objetivo de este tipo de ataque es manipular las tablas ARP de los diversos ordenadores de la red por medio de respuestas de ARP falsas para que, por ejemplo, un ordenador que está bajo el control del atacante actúe como punto de acceso inalámbrico o puerta de entrada para Internet.

[1] Man-in-the-Middle (MITM) Attacks: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks

3. Ataques basados en servidores DNS: cuando se utiliza un ataque de falsificación de DNS, el atacante intenta introducir información corrupta de caché de DNS a un host en un intento de acceder a otro host utilizando su nombre de dominio. Esto lleva a la víctima a enviar información confidencial a un host malicioso, con la creencia de que está enviando información a una fuente confiable.

-Herramientas/soluciones tecnológicas de ciberseguridad

1. Medida de seguridad básica pasa por proteger siempre los datos mediante un certificado SSL actualizado de una autoridad fiable. Son particularmente necesarios en páginas web que dispongan de acceso para usuarios registrados.
2. Ofrecer métodos adicionales de autenticación que permitan iniciar sesión de forma segura. Por ejemplo, con una autenticación multifactor a través del correo.
3. Como última medida de seguridad relacionada con la vulnerabilidad Man-in-the-middle, cabe mencionar el aviso al usuario de que nunca se les pedirá información confidencial a través de un correo electrónico.

DoS (Denegación de servicio): un ataque DoS[2] puede atacar a diferentes sistemas: RGPS, red, aplicaciones, IoT, etc. Su objetivo es provocar la falta de disponibilidad del sistema. La mayoría de los ataques DoS son causados por varias fuentes al mismo tiempo (por ejemplo, un número masivo de solicitudes enviadas por diferentes sistemas al mismo tiempo) enviadas al sistema de destino, también llamado Denegación de servicio distribuida (DDoS)[3]. Existen múltiples tipos de ataques basados en DoS, mostrándose a continuación cinco de los ataques más comunes:

a) Ataque de inundación UDP: es un tipo de ataque en el que se envía una gran cantidad de paquetes UDP a un servidor de destino con el objetivo de abrumar la capacidad de ese dispositivo para procesar y responder.
b) Ataque de inundación DNS: se inundan los servidores DNS de un dominio particular en un intento de interrumpir la resolución de DNS para ese dominio.
c) Ataque de inundación Ping (ICMP): se intenta abrumar a un dispositivo objetivo con paquetes de solicitud de eco ICMP, lo que hace que el objetivo sea inaccesible para el tráfico normal.

[2] DoS Attack: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
[3] DDoS Attack: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

d) Ataque de inundación HTTP: es un tipo de ataque diseñado para abrumar a un servidor objetivo con solicitudes HTTP. Una vez que el objetivo se ha saturado con solicitudes y no puede responder al tráfico normal, se producirá una denegación de servicio para solicitudes adicionales de usuarios reales.
e) Ataque de inundación SYN: abusa del TCP Threeway Handshake. Una conexión TCP siempre se establece con una autenticación completa de tres pasos. Para este propósito, el cliente envía un paquete de sincronización (SYN) al servidor. Cuando lo recibe, el servidor responde con un paquete de sincronización (SYN) y una confirmación (ACK). La conexión concluye con el acuse de recibo (ACK) por parte del cliente. En caso de que esta no se produzca, los sistemas se pueden paralizar, ya que el servidor no cuenta en su memoria con suficientes conexiones confirmadas. Si por medio de una inundación SYN se reúne un gran número de conexiones incompletas, los recursos disponibles del servidor se ocupan por completo.

-Herramientas/soluciones tecnológicas de ciberseguridad:

1. Usar listas negras para la identificación las direcciones IP críticas y el descarte de paquetes. Esta medida de seguridad puede ser implementada de forma manual o automática a través de las listas de bloqueo en el firewall (cortafuegos).
2. Limitar el número de solicitudes que un servidor aceptará durante un período de tiempo determinado, aunque por sí solo probablemente no sea suficiente para manejar un ataque DDoS complejo de manera efectiva.
3. No almacenar la información sobre los paquetes SYN en el servidor. En vez de guardarla se envía como una cookie encriptada al cliente. De esta forma un ataque de inundación SYN compromete la capacidad del sistema, pero no la memoria del sistema.
4. Utilizar una red Anycast para dispersar el tráfico del ataque a través de una red de servidores distribuidos. Al igual que canalizar un río que corre por canales más pequeños separados, este enfoque diluye el tráfico del ataque distribuyéndolo a través de múltiples servidores hasta un punto donde la red absorba el tráfico.
5. Por último, avances en filtrado de ingreso (IETF rfc2267) mediante el uso de iptables y sistemas de detección de

Intrusos de redes tales como snort pueden ayudar a rastrear y a evitar ataques DoS distribuidos.

IP spoofing (Suplantación de direcciones IP): la suplantación de IP[4] es la creación de paquetes de Protocolo de Internet (IP) que tienen una dirección de origen modificada para ocultar la identidad del remitente, suplantar a otro sistema informático o ambos. Es una técnica utilizada a menudo por atacantes para realizar ataques DDoS contra un dispositivo objetivo o la infraestructura circundante.

-Herramientas/soluciones tecnológicas de ciberseguridad:

1. Ingress filtering (filtrado de entrada)[5]. El ingress filtering es una forma de filtrado de paquetes que generalmente se implementa en un dispositivo periférico de red que examina los paquetes IP entrantes y examina sus encabezados de origen. Si los encabezados de origen de esos paquetes no coinciden con su origen o si se ven sospechosos, los paquetes se rechazan.

3.3 Ciberseguridad a nivel de Servidor

Acceso y privilegios a bases de datos mal definidos: un error importante de seguridad a nivel de servidor suele ser el uso de contraseñas predeterminadas, poco seguras o el exceso de privilegios de un usuario. Mediante un ataque por fuerza bruta se podría acceder a la base de datos. Por otra parte, un usuario con poco conocimiento de la gestión de la base de datos podría alterar alguna tabla por un exceso de privilegios en su usuario.

- Soluciones:
  1. Crear distintos roles de usuario y asignarles distintos privilegios[6] (lectura, escritura, administrador, etc…) en función de las necesidades[7].
  2. Es muy recomendable aislar la base de datos de la red pública mediante direccionamiento privado. Solo el servidor API debería tener acceso directo a la base de datos.
  3. Las credenciales y los privilegios[8] deben ser revisados periódicamente y se debe limitar el número de reintentos de accesos erróneos consecutivos en un intervalo de tiempo,

[4] Ip-spoofing: https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/
[5] Ferguson, P.; Senie, S. "BCP 38" https://tools.ietf.org/html/bcp38, May 2000
[6] Villalobos J., 'Vulnerabilidad de sistemas gestores de bases de datos',UNICIENCIA 22 pp. 131-134 , 2008
[7] Robert W., 'Naming and Grouping Privileges to Simplify Security Management in Large Databases',Tandem Computers

de esta forma el sistema será más robusto contra ataques DDoS.

Cuentas y contraseñas de usuario inseguras y perfiles de usuario mal definidos: es crucial el uso de contraseñas seguras en los usuarios del sistema para evitar el acceso de un usuario no autorizado o la edición de archivos críticos. No deben ser accesibles archivos críticos del sistema a todos los perfiles de usuario y al igual que los usuarios de base de datos, una contraseña insegura es susceptible a ataques por fuerza bruta.

-Herramientas/soluciones tecnológicas de ciberseguridad:

Uno de los puntos más básicos e importantes de un sistema es evitar el uso de contraseñas inseguras[9] y actualizarlas periódicamente. Una contraseña segura previene de ataques de usuarios malintencionados que utilizan contraseñas por defecto o realizan ataques por fuerza bruta.

Es también muy recomendable utilizar passphrases[10] en los servidores en lugar de contraseñas.

Proteger el acceso a directorios según roles de usuario es indispensable para la seguridad de cualquier sistema e impide la ingesta de código de un usuario malintencionado.

Otra posible solución puede ser usar un protocolo de acceso es LDAP[11] (Protocolo Ligero de Acceso a Directorio)[12] en el que hay distintos niveles de acceso y permisos de usuario para la estructura de archivos.

Mala configuración de nombres de dominio y certificados SSL: la ausencia o mala configuración de los certificados ssl[13] en los servidores hace que la comunicación cliente-servidor sea insegura y sea susceptible a ser analizada por un sniffer para obtener información sensible tanto del usuario como del servidor o la base de datos.

- Herramientas/soluciones tecnológicas de ciberseguridad:

El servidor debe utilizar certificados ssl seguros por una autoridad confiable como podría ser VeriSign, GeoTrust, Cómodo. Este debe asociarse al nombre de dominio del servidor y ha de habilitarse el tráfico

[9] Wayne C. Summers & Edward Bosworth, 'Password policy: the good, the bad, and the ugly', WISICT'04, 2004
[10] Keith M. & Shao B. & Steinbart P., 'The usability of passphrases for authentication: An empirical field study', ScienceDirect, 2007
[11] Donnelly M., 'Una Introducción a LDAP'
[12] Zeilenga K., 'Lightweight Directory Access Protocol: Technical Specification Road Map', 2006
[13] Freier A. & Karlton P. & Kocher P., 'The Secure Sockets Layer (SSL) Protocol Version 3.0', 2011

HTTPS[14] para que los clientes que le hacen solicitudes empleen una comunicación cifrada.

Para evitar usar el protocolo inseguro HTTP, este debe bloquearse al menos para uso por direccionamiento público. Otra posible solución sería redireccionar el acceso HTTP a HTTPS en el inicio de la aplicación.

Software desactualizado o sin licencia: el uso de aplicaciones o sistemas operativos desactualizados permite que los hackers aprovechen las vulnerabilidades conocidas y ya solventadas del sistema para acceder a la información del servidor. Entrando en un nodo con esta vulnerabilidad podrían ser capaces de acceder a otros nodos de la red.

- Herramientas/soluciones tecnológicas de ciberseguridad:

Las actualizaciones en los sistemas operativos o aplicaciones suelen contener parches de seguridad que solucionan vulnerabilidades conocidas[15]. Es importante actualizar los programas a la última versión o estos huecos de seguridad para acceder al sistema.

Firewall desconfigurado (Sistema operativo): al utilizar puertos por defecto en los servicios o protocolos, es más probable que los servicios reciban ataques directos comunes. Es importante limitar el acceso al servidor solo a los puertos e ips de hosts ya conocidos en caso de ser posible. El uso de protocolos no seguros permite el acceso a información sensible a los usuarios no autorizados.

-Herramientas/soluciones tecnológicas de ciberseguridad:

1. Evitar usar puertos por defecto[16] en la medida de lo posible en cada uno de los servicios.
2. Configurar correctamente iptables[17] y crear una lista blanca/negra de ips y puertos.
3. Se debe limitar el acceso a directorios con información crítica que solo deben ser accesibles por un administrador.
4. Bloquear puertos e ips que no deban tener acceso, así como los protocolos que no se utilicen o los inseguros.
5. Bloqueo del protocolo ICMP (ping) para evitar ataques DDoS o sniffing e intentar pasar desapercibido ante posibles ataques.

[14] Durumeric Z. & Kasten J. & Bailey M. & Halderman J., 'Analysis of the HTTPS certificate ecosystem', IMC'13, 2013
[15] Kagan A. 'Computer security and operating system updates', ScienceDirect, 2003
[16] William R. & Kevin E., 'Enterprise Considerations for Ports and Protocols', Institute for Defense Analysis, 2016
[17] Diekmann C. & Michaelis J. & Haslbeck M. & Carle G., 'Verified iptables firewall analysis', IEEE Xplore, 2016

6. Es crítico usar protocolos seguros en la medida que se pueda HTTPS en lugar de HTTP, FTPS en lugar de FTP, SSH en lugar de Telnet, SMTPS en lugar de STMP, etc.

Ataques de malware: malware es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas. Algunos de los más críticos son los virus, gusanos, troyanos y uno bastante común actualmente, el ransomware[18] (un tipo de malware que restringe el acceso a determinadas partes del sistema operativo infectado y pide un rescate a cambio).

-Herramientas/soluciones tecnológicas de ciberseguridad:

Las principales técnicas contra los ataques malware son:

1. Disponer un sistema de copias de seguridad[19] aislado de accesos públicos gracias al que el sistema podrá restaurarse rápidamente en caso de encriptación.
2. Actualizar continuamente el sistema y los programas a la última versión disponible, aprovechando los nuevos parches de seguridad que solucionan problemas detectados.
3. Formar y concienciar a los usuarios para que sepan identificar los ataques y prevenirlos.

Deficiencia en la monitorización del servidor: aun habiendo configurado correctamente el servidor es interesante mantener el servidor constantemente monitorizado para poder detectar problemas o ataques a tiempo real. Los ataques están en evolución contante y es necesario registrar lo que sucede en el sistema para poder analizarlo y actuar o incluso realizar un análisis forense para localizar la autoría del ataque.

-Herramientas/soluciones tecnológicas de ciberseguridad:

Es necesario registrar las solicitudes que pueda recibir el servidor y poder visualizarlas a tiempo real. Un ejemplo de solución en este sentido podría ser nagios (open source log server). Es una herramienta open source de monitorización IT que proporciona monitorización, alertas, reportes y gráficas acerca del sistema.

3.4 Ciberseguridad a nivel de Aplicación

Cross Site Scripting: es un tipo de inyección que permite que un atacante inserte código malicioso en aplicaciones benignas y de confianza. Este

[18] O'Gorman G. & McDonald G., 'Ransomware: A Growing Menace', Symantec Security Response
[19] Thomas J. & Galligher G., 'Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware', SSRN, 2018

código es normalmente un script del lado del navegador web que el atacante hace llegar a otro usuario final de la aplicación. El usuario no tiene forma de saber que el script no es originario de la app web. Estos scripts pueden incluso reescribir el contenido HTML Esto permite al atacante acceder a cookies, tokens de sesión y cualquier otra información sensible contenida en el navegador. Este artículo de Alecu F[20]. explica en detenimiento este tipo de vulnerabilidad.

-**Herramientas/soluciones tecnológicas de ciberseguridad:**

Hay algunas etiquetas HTML que se pueden usar para transmitir un script malicioso. La solución básica consiste en hacer una revisión del código, para identificar los lugares donde un input, que realiza una petición HTTP, pudiera abrirse camino hasta la salida HTML, en estas etiquetas mencionadas. Hay herramientas disponibles como Nessus o Nikto que pueden ayudar a identificar estas vulnerabilidades.

SQL Injection: inserción de una query SQL en una entrada de datos del usuario en la aplicación. Esto permite, ya no sólo obtener datos de la BBDD, sino también realizar operaciones (Insert/Update/Delete), así como realizar acciones de administrador en la BBDD.

-Herramientas/soluciones tecnológicas de ciberseguridad:

Una solución básica es crear una "whitelist" de caracteres permitidos en formularios, de forma que el atacante no pueda escribir cualquier cosa en el campo de entrada. Por otro lado, la mayoría de los sistemas gestores de BBDD permiten usar "Stored Procedures", que son instrucciones SQL preestablecidas en la BBDD que admiten parámetros, de forma que la aplicación no lanza la query, directamente, sino que llama al procedimiento, impidiendo que el atacante realice ninguna otra operación que no sea la que está establecida.

Broken Authentication: capacidad de un atacante para acceder con las credenciales de otro usuario, de forma no autorizada [2122] .

- Herramientas/soluciones tecnológicas de ciberseguridad:

1. Para corregir las vulnerabilidades en la autenticación de usuarios, hay un amplio abanico de acciones realizables. Como medida inicial, la aplicación no debe permitir que los usuarios establezcan

[20] https://www.researchgate.net/publication/241757130_Cross_Site_Scripting_XSS_in_Action

[21] Hassan M, Sultana S., Akter M., Haque R., 'Broken Authentication and Session Management Vulnerability: A Case Study of Web Application', International Journal of Simulation: Systems, Science & Technology, 2018

[22] https://dzone.com/articles/broken-authentication-and-session-management-part

contraseñas débiles, o de uso común. Estas contraseñas no deben enviarse al servidor en texto plano o con una encriptación débil. Siguiendo con medidas para la contraseña, si un usuario la olvida, es necesario que el proceso para recuperarla sea seguro y de garantías. Por ejemplo, habría que evitar las preguntas de seguridad que pudieran tener una respuesta previsible o fácilmente adivinable.

2. Como medidas más profundas, es preferible utilizar una autenticación multi-factor, y usar un gestor de sesión seguro del lado del servidor, que genere ID's aleatorias tras el login. También se pueden tomar medidas adicionales para impedir que se realicen ataques de fuerza bruta, o de diccionario, donde un atacante automatiza un proceso en el que se van probando secuencialmente usuarios y contraseñas.

Information Disclosure: la aplicación falla a la hora de proteger con garantías la información sensible o confidencial, de atacantes que no deberían tener acceso a la misma. Esta vulnerabilidad no causa daños per se, pero permite a los atacantes acceder a información que más tarde puede usarse en el "ciclo de vida del ataque", permitiendo hacer más daño del que podrían si no dispusieran de esta información. También hay que considerar el daño en cuanto a la privacidad, o económico que puede derivarse del acceso a esta información[23].

-Herramientas/soluciones tecnológicas de ciberseguridad:

Lo primero es adoptar las medidas que garanticen un control de acceso y una autenticación robusta. Después es necesario llevar a cabo acciones como no permitir que el servidor incluya información en los headers de sus respuestas, sobre la tecnología del backend o la versión, o no permitir que los servicios que se ejecutan en puertos abiertos del servidor revelen información sobre las "builds" o versiones. Se deben gestionar correctamente los errores de la aplicación, para que no muestren información técnica. Así mismo, se debe mostrar una pantalla de error genérica en aquellos recursos deshabilitados o inexistentes. Algo esencial, también, es suprimir del código cualquier contraseña, API Key, dirección IP o cualquier otra información sensible. Por último, en cuanto al servidor, no debe listar el contenido de los directorios. Ni tampoco alojar información o ficheros que no sean necesarios para el funcionamiento de la aplicación[24] .

[23] He S., Moo G., Han S., Whinston A., 'How would Information Disclosure influence organizations' outbound spam volumen? Evidence from a field experiment', Journal of Cybersecurity, Volume 2, Issue 1, 2016

[24] https://www.netsparker.com/blog/web-security/information-disclosure-issues-attacks/

Privilege escalation: muchas aplicaciones web se basan en el concepto de que cada usuario puede realizar unas acciones determinadas en función de los privilegios que tiene asignados. "Privilege escalation" es el hecho de que un usuario (o sistema, u otra aplicación) pueda acceder a recursos, o realizar acciones que no le corresponden por su rol de usuario y los privilegios que le corresponden. Esto puede ocurrir vertical u horizontalmente: Se denomina escalada de privilegios vertical si un usuario lleva a cabo acciones que tienen privilegios por encima de su nivel. Mientras que se llama 'horizontal' en el caso de un que un usuario pueda acceder al rol de otros usuarios que están a su mismo nivel.
Se puede encontrar más información detallada sobre la escalada de privilegios en las webs de OWASP[25] y netwrix[26].

-Herramientas/soluciones tecnológicas de ciberseguridad:

Una medida básica es transversal a varias de las vulnerabilidades expuestas, esto es la correcta validación del control de usuarios y autenticación. Por otra parte, es necesario revisar qué puede hacer, o a qué recursos puede acceder cada usuario, otorgándole a cada rol sólo lo mínimo necesario para el correcto funcionamiento de la aplicación[27][28].

Server side request forgery: vulnerabilidad de una aplicación mediante la cual, el atacante puede acceder o modificar recursos del propio servidor. El atacante, típicamente provee o modifica una URL cuyo código es leído por el servidor, exponiendo configuración de este, o accediendo a servicios internos. El atacante podría llevar a cabo peticiones POST a servicios internos que no están expuestos de forma pública.[29],[30],[31] y[32].

-Herramientas/soluciones tecnológicas de ciberseguridad:

1. En primer lugar, se debe utilizar una "whitelist" de dominios y protocolos permitidos, desde los cuales el servidor puede obtener recursos remotos. Se debe evitar, también, la entrada de datos directa del usuario en aquellas funciones que puedan hacer peticiones en nombre del servidor.

---

25 https://owasp.org/www-community/vulnerabilities/Least_Privilege_Violation

26 https://blog.netwrix.com/2018/09/05/what-is-privilege-escalation/

27 Provos N., Friedl M., Honeyman P., 'Preventing Privilege Escalation', 12th USENIX Security Symposium, 2003

28 Jaafar F., Nicolescu G., Richard C., 'Systematic Approach for Privilege Escalation Prevention', IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2016

29 https://owasp.org/www-community/attacks/Server_Side_Request_Forgery

30 https://portswigger.net/web-security/ssrf

31 https://www.netsparker.com/blog/web-security/server-side-request-forgery-vulnerability-ssrf/

32 https://www.hackerone.com/blog-How-To-Server-Side-Request-Forgery-SSRF

2. Establecer un servicio intermedio entre el front end y el back end, para controlar con más exactitud qué llega al servidor.

-Herramientas de detección automática de vulnerabilidades:

En la actualidad, existen herramientas de detección automática de vulnerabilidades de aplicaciones web. Para el caso de estudio de este proyecto, son relevantes aquellas con política de software libre y código abierto como Grabber21, Zed Attack Proxy22, Wapiti23, W3af24 o X5S25. Se ha de tener en cuenta que estas herramientas o aplicaciones no son de propósito general y no cubren por sí solas, todo el amplio espectro de vulnerabilidades conocidas que pueden afectar a una aplicación

4. Tendencias

4.1 Literatura científica

Survey on Man in the Middle Attack

Autor: Jain, K. M., Jain, M. V., & Borade, J. L

Publicado en: 2016. *IJSTE-International J. Sci. Technol. Eng, 2(09), 277-280.*

Abstract:
The de-facto standards of the security protocol SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are used to create a connection between two clients or web service which is secure and stable [1]. Man in the middle attack allows the attacker to gain unauthorized entry into the connection between two devices and listen to the network traffic. This type of attack is very fatal because it is almost invisible to the victim device. This survey paper on man in the middle attack focuses on the execution of man in the middle attack on Diffie-Hellman and what are the different methods with which it can be performed and the various defenses against the attack.

A taxonomy of DDoS attack and DDoS defense mechanisms

Autor: Mirkovic, J., & Reiher, P.

Publicado en: 2004. ACM SIGCOMM Computer Communication Review, 34(2), 39-53. DOI: 10.1145/997150.997156

Abstract:
Distributed denial-of-service (DDoS) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. This paper presents two taxonomies for classifying attacks and defenses, and thus provides researchers with a better understanding of the problem and the current solution space. The attack classification criteria was selected to highlight commonalities and important features of attack strategies, that define challenges and dictate the design of countermeasures. The defense taxonomy classifies the body of existing DDoS defenses based on their design decisions; it then shows how these decisions dictate the advantages and deficiencies of proposed solutions.

A Survey of Defence Mechanisms against IP Spoofing

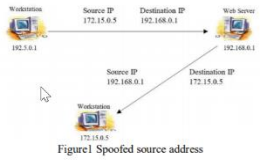

Figure1 Spoofed source address

Autor: Sahni S. & Jasgtap P.

Publicado en: 2017. *IARJSET, 4*(7), 20-27.; doi: 10.17148/IARJSET.2017.4704

Abstract:
IP address spoofing is a serious threat to the legitimate use of the Internet. Many Preventive mechanisms are thwarted by the ability of attackers to forge or spoof the source addresses in IP packets. Attackers can evade detection and put a substantial burden on the destination network for policing attack packets. In this paper a study of methods for detection of IP address spoofing is undertaken. It compares various host based methods such as IPSec, the OS Fingerprinting, TCP probing, SYN Cookies and IP puzzles with router based methods such as ingress and egress filtering, Reverse Path Forwarding (RPF), Router based Filtering (RBF), Spoofing Prevention Method (SPM), Distributed Packet Filtering (DPF), Inter Domain Packet Filtering (IDPF), SAVE, BASE, Hop Count Filtering (HCF), Pi and StackPi on the bases of their performances and effectiveness.

VULNERABILIDAD DE SISTEMAS GESTORES DE BASES DE DATOS

Autor: Villalobos Murillo, J.

Publicado en: 2008. *UNICIENCIA, 22.*

Abstract:
Existe una constante preocupación por la segu-ridad de las bases de datos; muchas veces la seguridad se ve afectada por la configuración de los procesos de conexión. En este ensayo se estudia como se configuran las conexiones hacia una base de datos, explicando los posibles errores y se proporcionan recomendaciones para disminuir el riesgo asociado a estos procesos.

Naming and Grouping Privileges to Simplify

Autor: Baldwin W., Robert.

Publicado en: 1990. IEEE Symposium on Security and Privacy (pp. 116-132).

Abstract:
This paper describes an extension to ANSI SQL that simplifies security management by reducing the complexity of the access controls on database objects, and by providing users with the flexibility to define administrative roles (like Auditor or Security Administrator) that match their requirements for the separation duties. The benefit of simplified security management is improved security. The main features of extension have been adopted for a future version of the ANSI SQL standard. This paper focuses on major concepts and issues, not syntax and implementation. The key idea is to allow users to group and name privileges to form named protection domains (NPDs). The Clark-Wilson and Bell-LaPadula models are used to illustrate the benefits and limitations of NPDs. The main conclusion is that the naming and abstracting mechanisms provided by NPDs can simplify security management in much the same way that procedures can simplify programming.
The SQL security system is based on access control lists (ACLs). Rach ACL indicates which individuals can perform each operation. The current ANSI SQL standard does not include the ability to grant privileges to groups of individuals. Another feature of the standard is that most operations can be granted to tother users, but some, like adding a new column to a table, can only be performed by the object's owner. A privilege (an operation-object pair) can be granted with grant option", which allows the recipient to pass that privilege on to other users, including the

possibility of allowing the other users to further grant the privilege. A SQL data dictionary table records who granted which privileges to whom. Privileges are taken away from users with the revoke statement. One option of revoke is to cascade the removal of privileges to cover the case where the original recipient has passed on the privileges. The rules that govern cascading revocating are complex, and like any complex control system chosen and fixed by vendors, only a few customers will find that it meets their needs.

Password policy: the good, the bad, and the ugly

Autor: Password policy: the good, the bad, and the ugly

Publicado en: 2004. Proceedings of the winter international synposium on Information and communication technologies (pp. 1-6).

Abstract:
"We're secure! We use passwords!" How many of us have heard this claim? Or even – "We're secure! We have a password policy!" Using a password or having a password policy in today's world of computing is not enough. Passwords provide a first line of defense in most cases, but there is much more. "A recent survey by Rainbow Technologies Inc. indicates that the use of insecure passwords can be costly -- and potentially risky – for corporate data."[Rosencrance] This paper focuses on the use of passwords and password policy and looks at the good, the bad and the ugly scenarios that arise.

The usability of passphrases for authentication: An empirical field study.

International Journal of Human-Computer Studies
www.elsevier.com/locate/ijhcs

Autor: The usability of passphrases for authentication: An empirical field study.

Publicado en: 2007. International journal of human-computer studies, 65(1), 17-28. DOI: 10.1016/j.ijhcs.2006.08.005

Abstract:
In developing password policies, IT managers must strike a balance between security and memorability. Rules that improve structural integrity against attacks may also result in passwords that are difficult to remember. Recent technologies have relaxed the 8-character password constraint to permit the creation of longer pass-"phrases" consisting of multiple words. Longer passphrases are attractive because they can improve security by increasing the difficulty of brute-force attacks and

they might also be easy to remember. Yet, no empirical evidence concerning the actual usability of passphrases exists. This paper presents the results of a 12-week experiment that examines users' experience and satisfaction with passphrases. Results indicate that passphrase users experienced a rate of unsuccessful logins due to memory recall failure similar to that of users of self-generated simple passwords and stringent passwords. However, passphrase users had more failed login attempts due to typographical errors than did users of either simple or highly secure passwords. Moreover, although the typographical errors disappeared over time, passphrase users' initial problems negatively affected their end-of-experiment perceptions.

An introduction to LDAP

Autor: Donnelly, M.

Publicado en: Obtained from http://www. ldapman. org/articles/intro_to_ldap. html.

Abstract:
Para empezar con ello, lo que está ocurriendo con LDAP hoy es novedoso. Una implementación a lo largo de la empresa puede facilitar la obtención de información de tu directorio LDAP a casi cualquier aplicación, ejecutándose en cualquier plataforma de computación . Y en teoría puede ser utilizada para almacenar un amplio rango de datos: dirección de correo electrónico e información de encaminamiento de correo, datos de RRHH, claves publicas de seguridad, listas de contactos, y mucho más. Haciendo un directorio LDAP un punto de enfoque en tu integración de sistemas, estas proveyendo de un almacén de 'única parada' para cualquier persona que busque información dentro de tu empresa - incluso si la fuente primaria de datos reside en cualquier otro lugar.

Lightweight directory access protocol (ldap): Technical specification road map

Autor: Zeilenga, K.

Publicado en: 2006. RFC 4510

Abstract:
The Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing distributed directory services that act in accordance with X.500 data and service models. This document provides a road map of the LDAP Technical Specification.

The secure sockets layer (SSL) protocol version 3.0

Autor: Freier, A., Karlton, P., & Kocher, P.

Publicado en: 2011. IETF, 3, 1-67.

Abstract:
This document is published as a historical record of the SSL 3.0 protocol. The original Abstract follows.

This document specifies version 3.0 of the Secure Sockets Layer (SSL3.0) protocol, a security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to preventeavesdropping, tampering, or message forgery.

Computer security and operating system updates

Autor: Post, G., & Kagan, A.

Publicado en: 2003. Information and Software Technology, 45(8), 461-467. DOI: 10.1016/S0950-5849(03)00016-8

Abstract:
Application and operating system errors are a continuing source of problems in computer security. As businesses increase the number of servers through distributed computing and server farms, it becomes more difficult to keep the systems up to date. A survey of security professionals reveals that most find it difficult to keep up to date with security patches. Consequently, developing more automated management tools is an important step in improving enterprise security

Enterprise considerations for ports and protocols

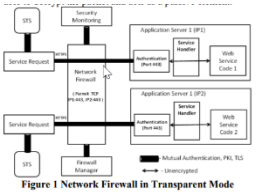
Figure 1 Network Firewall in Transparent Mode

Autor: Foltz, K. E., & Simpson, W. R.

Publicado en: 2016. Institute for Defense Analyses Alexandria.

Abstract:
The need to control information flow to a restricted set of accepted protocols arises from the vulnerabilities that may come from any protocol. Reducing the acceptable protocols to

a small set of well-tested standard protocols will reduce the attack surface and provide high confidence in selected communications. These protocols are restricted to specific ports or addresses in the receiving web service. HTTPS is familiarly restricted to port 443. In the standard nomenclature, this traffic may be configured as either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). The standard ports are defined by Internet Assigned Numbers Authority (IANA). The IANA is responsible for maintaining the official assignments of port numbers for specific uses. However, many unofficial uses of both well-known and registered port numbers occur in practice. Screening of acceptable ports and protocols has been done, in the past, by network appliances known as firewalls. Communications on the approved list were permitted, others blocked. However, many appliances now have such functionality and the server or service may have a host-based security system that can apply this functionality. This paper covers enterprise considerations for screening of ports and protocols.

Verified iptables firewall analysis

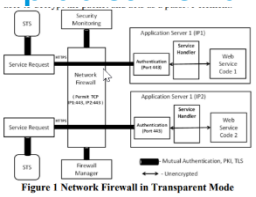

Figure 1 Network Firewall in Transparent Mode

Autor: C. Diekmann, J. Michaelis, M. Haslbeck and G. Carle

Publicado en: 2016. IFIP Networking Conference (IFIP Networking) and Workshops. pp. 252-260. DOI: 10.1109/IFIPNetworking.2016.7497196.

Abstract:
We present a fully verified firewall ruleset analysis framework. Ultimately, it computes minimal service matrices, i.e. graphs which partition the complete IPv4 address space and visualize the allowed accesses between partitions for a fixed service. Internally, we are working with a simplified firewall model and a core contribution is the translation of complex real-world iptables firewall rules into this model. The presented algorithms and translation are formally proven correct with the Isabelle theorem prover. A real-world evaluation demonstrates the applicability of our tool. Both the iptables-save datasets and the Isabelle formalization are publicly available.

4.2 Proyectos

THREAT-ARREST Cyber Security Threats and Threat Actors Training - Assurance Driven Multi-Layer, end-to-end Simulation and Training

Financiado por: Horizon 2020

Periodo de financiación: 2018/2021

+ INFO

Resumen:

THREAT-ARREST aims to develop an advanced training platform incorporating emulation, simulation, serious gaming and visualization capabilities to adequately prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk cyber systems and organizations to counter advanced, known and new cyber-attacks. The THREAT-ARREST platform will deliver security training, based on a model driven approach where cyber threat and training preparation (CTTP) models, specifying the potential attacks, the security controls of cyber systems against them, and the tools that may be used to assess the effectiveness of these controls, will drive the training process, and align it (where possible) with operational cyber system security assurance mechanisms to ensure the relevance of training. The platform will also support trainee performance evaluation and training programme evaluation and adapt training programmes based on them. The effectiveness of the framework will be validated using a prototype implementation interconnected with real cyber systems pilots in the areas of smart energy, healthcare and shipping, and from technical, legal and business perspectives.

The THREAT-ARREST platform will offer training on:
a) known and new advanced cyber-attack scenarios
b) use of different security tools for detecting and/or responding to cyber-attacks
c) taking different types of actions against cyber-attacks
d) use of security testing, monitoring and assessment tools at different layers (network, infrastructure, application) in a cyber system

The project's objectives include:

- Develop the means for specifying cyber security threat training and preparation models and programs to drive the realization of the training process
- Develop emulation capabilities enabling the creation of virtual cyber system components, subjecting them to cyber-attacks for training purposes, and enabling trainees to take appropriate response actions and hands-on experience against these cyber-attacks
- Develop multi-layer simulation capabilities enabling the realistic simulation of cyber systems, their usage and security attacks launched on them, through synthetic events at all layers in the implementation stack of these systems and their components reflecting realistic system conditions
- Develop cyber-security training based on serious games and enable trainees to get engaged in cyber-defence, elicit threats and learn about attacks
- Develop key capabilities for the effective delivery of CTTP programs, i.e. the visualization of the operation and state of cyber systems and the emergence and effects of attacks against them; assessing trainee performance in CTTP programs and adapting them depending on it; and assessing the overall effectiveness of a CTTP program and evolving it accordingly
- Align training and simulation with the continuous security assurance of real operational cyber systems, by integrating the developed capabilities into a common platform together with security assurance assessment capabilities
- Demonstrate the use of the THREAT-ARREST framework for effective training against cyber-attacks in the domains of smart energy, healthcare and transport (shipping), using real operational cyber systems within these domains as pilots and, through them, evaluate and validate the framework
- Ensure the uptake, commercialization, and the delivery of innovation of project outcomes by developing an ecosystem around the THREAT-ARREST framework.

COmpetitive Methods to protect local Public Administration from Cyber security Threats

COMPACT
CYBERSECURITY FOR PUBLIC ADMINISTRATIONS

Financiado por: Horizon 2020

Periodo de financiación: 2017/2019

+ INFO

Resumen:

"The cybersecurity landscape is changing, and Local Public Administrations (LPAs) are now an attractive target for cybercriminals. Cyber-attacks against local governments have become very common and the consequences may include disclosure of personal data, or gain control over smartly operated city resources through LPAs infrastructures, thus significantly impacting both individuals and organisations.

COMPACT works to address these issues by empowering local LPAs to become the main actors of their cyber-resilience improvement process and by providing them with effective tools and services for removing security bottlenecks. This is done by (#1) Making the PA personnel aware of the basic cyber security threats they are exposed to (#2) Improving the skills – both technical and behavioural – of the PA personnel via innovative training techniques that are well received by the (non IT-expert) workforce (#3) Providing protection tools against basic cyber security threats, i.e. those with a higher impact on LPAs. These include phishing, ransomware, Bring Your Own Device (BYOD) and more (#4) Creating a LPAs level information hub, for favouring reliable and timely exchange of information among LPAs on cyber security guidelines and best practices, as well as on Indicators of Compromise (IoC) and (#5) Creating a link between COMPACT LPAs level information hub and major EU level initiatives, for supporting LPAs to improve cyber-resilience in a complex European context.

To achieve its objectives, COMPACT is developing four types of tools/services, which include: (1) Risk assessment tools - enabling LPAs to evaluate and monitor their exposure to the most relevant cyber treats to prioritize the adoption of preventive and reactive countermeasures for maximum efficiency of resource usage for cyber protection purposes (2) Education services - through dedicated game-based training, focused not only on specific cyber-threats but also on psychological and behavioural factors, to maximize the effectiveness of the learning experience, while also containing the training time (3) Monitoring services – that continuously process events related to the status of the infrastructure and correlate them with information from threat intelligence feeds to timely spot anomalies and also suggest recovery actions that can be implemented (4) Knowledge Sharing services – including best practices and guidelines, focused on the specific needs of LPAs, that can be easily adopted to quickly increase the cyber security level of the organization."

Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things

Financiado por: Horizon 2020

Periodo de financiación: 2018/2021

+ INFO

Resumen:

The security problems arising, in Internet of Things (IoT) ecosystems, from the flawed design of legacy hardware and embedded devices, the lack of processing and storage capacity (among other) allows cyber-criminals to easily compromise these devices and launch large-scale attacks towards critical cyber-infrastructures or intercept personal data. The Cyber-Trust project aims to develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform which will safeguard heterogenous ecosystems of IoT devices. To achieve this goal, Cyber-Trust will follow interdisciplinary approach in order to capture the different phases of such emerging threats, before, at the time and after known or unknown vulnerabilities have been exploited by cyber-criminals. The proposed cyber-security platform, which is under development in the Cyber-Trust framework, will enhance the safety and security of the digital assets of citizens (e.g. Smart Homes, wearable devices, baby monitor, thermostat, mobile devices etc.) and organisation's infrastructure (e.g. smart building, sensors and actuators).
Furthermore, as most of these devices, hold and transmit a huge amount of personal and sensitive data, through multiple heterogenous networks, the protection and early warning of the users regarding the state of the devices of EU citizens is of the highest importance.
Addressing and developing a solution regarding the aforementioned challenging areas, is undoubtedly a matter of high importance, since the IoT systems applied in all the aspects of our daily life.

A cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

Financiado por: Horizon 2020

Periodo de financiación: 2019/2022

+ INFO

Resumen:

The telecommunications sector is very vulnerable to cyberattacks. Despite billions of euros invested in cybersecurity measures, cyberattack mechanisms are becoming increasingly sophisticated, pervading critical infrastructures. The EU-funded SPIDER project plans to deliver an innovative cyber range platform that extends and combines the capabilities of existing telecommunication testbeds and cyber ranges into a unified facility. The virtual environment will be used for help train information security professionals to deal with real-world incidents, test new security technologies, and support companies in making optimal cybersecurity investment decisions. The gamification feature will make keep training exciting and increase the collaborative ability in handling incidents and defending against cyberattacks.

Bringing to the market a new generation of AI-powered Media Monitoring Tools

Financiado por: Horizon 2020

Periodo de financiación: 2021/2023

+ INFO

Resumen:

Media Monitoring is the systematic recording of media output related to a specific target, its activities and topics of interest. With the galloping growth of sources, many media monitoring companies have addressed this issue by increasing human resources. However, human expertise which should be focused in advanced analysis is being wasted on time-consuming mechanical tasks.

Current commercial solutions peddle the use of "Artificial Intelligence", but they are still highly dependent on human expertise to filter out irrelevant content. The worldwide market for media monitoring is valued at US$2.23 bn (2017), with a CAGR of 13,6% until 2022.

Building on 3 years of cutting-edge AI research funded by H2020, Priberam is developing a real-time crosslingual global media monitoring platform that delivers actionable insight beyond human

capabilities. Our system, based on a scalable SaaS business model, continuously ingests massive multilingual data sources and automatically translates, filters, categorizes and generates reports for media monitoring professionals.

MONITIO will be co-created with end-users at Deutsche Welle and improved with cutting-edge technology from Cambridge University, focusing on GDPR and the new EU Copyright legislation, making it the first media monitoring tool copyright compliant-by-design (in opposition to the majority of competitor solutions, which are US-based and not centred in these issues).
Priberam is a Portuguese SME that provides cutting-edge Natural Language Understanding and Artificial Intelligence technologies to companies in the media, legal and healthcare industries, and exports its technologies to international top companies such as Microsoft, Amazon, Kobo, and the main media publishers in Portugal, Spain and Brazil. Our team of 24 generated a turnover of 1,4M€ in 2018.

We believe that MONITIO will bring Media Monitoring to a new disruptive level, and place European technology in the lead of AI-powered Media Monitoring services.

4.3 Noticias

El valor de la ciberseguridad: "Un ataque hace desaparecer al 60% de las empresas"

Publicado en: Bolsamanía

Fecha: 01/11/2020

El confinamiento provocado por la crisis del coronavirus ha hecho que pasemos muchas horas delante de dispositivos electrónicos. Ha crecido el ecommerce, pero también los ataques cibernéticos. El más dañino es el 'ransomware', y su vía de entrada suele ser el 'phishing' (mail con intenciones maliciosas) con el que los ciberdelincuentes tratan de acceder a los sistemas informáticos. Es tan peligroso que el 60% de las empresas que sufren un ataque de este estilo desaparecen a los seis meses…

Ver noticia

Descubren una campaña de "malware" por email que suplanta al Ministerio de Trabajo y Economía Social

Publicado en: Portal Tic

Fecha: 21/08/2020

Descubren una campaña de 'malware' por email que suplanta al Ministerio de Trabajo y Economía Social.
El Instituto Nacional de Ciberseguridad (Incibe) ha alertado sobre el descubrimiento de una campaña de distribución de 'malware' por correo electrónico que de hace pasar por el Ministerio de Trabajo y Economía Social. Esta amenaza, que se ha descubierto este jueves, está integrada por una "campaña masiva" de correos electrónicos fradulentos cuya intención en realidad es difundir 'malware', por lo que se ha valorado como de importancia alta -cuatro en una escala de cinco-, como ha informado INCIBE en su página oficial…

Ver noticia

Ciberataques en tiempos de pandemia

Publicado en: Newtal

Fecha: 08/10/2020

En un mundo cada vez más digital, el espacio que se abre entre servidores, cables y satélites es campo de ciberataques, y el año de la pandemia no iba a ser la excepción. Más bien, todo lo contrario.

Durante los últimos años los informes del Centro Nacional de Inteligencia (CNI) han ido registrando aumentos de los ciberincidentes. Estas intrusiones o ataques afectan a empresas, administraciones del estado y particulares, y van desde intrusión en redes o equipos, hasta secuestro de datos personales, ataques con malware, phishing o otro tipo de fraudes...

Ver noticia

Artificial Intelligence and ML in cybersecurity: is it worth the hype?

Publicado en: Analytics Insight

Fecha: 30/09/2020

The world is going digital at a pace faster than the blink of an eye. Artificial intelligence (AI) and machine learning (ML) have been heralded as a means of digital technology that can solve a wide range of problems in different industries and applications. This also includes the realm of cybersecurity. Capgemini's Reinventing Cybersecurity with Artificial Intelligence Report, which was published last year, found that 61% of enterprises say they cannot detect breach attempts today without using AI technologies…

Ver noticia

<<He visto a directivos llorando, literalmente, por haber perdido sus archivos en un ciberataque>>

Publicado en: ABC

Fecha: 19/10/2020

Ciberguerra, ciber milicias, ataques teledirigidos. Centenares de virus informáticos que asolan a las infraestructuras. El campo de la seguridad informática es muy amplio y cada vez más importante para la economía y las empresas. Con las medidas de confinamiento adoptadas durante la pandemia, miles de compañías han adoptado el teletrabajo como alternativa para mantener sus actividades, pero esto ha dejado expuestos datos sensibles. Lorenzo Martínez (Logroño, 1978), perito informático forense y fundador de la empresa de ciberseguridad Securízame, señala en una entrevista a ABC realizada por videconferencia las posibles vulnerabilidades de estas formas productivas llamadas a extenderse en el futuro y otras tendencias en este sector al auge…

Ver noticia

INCIBE lanza una guía de ciberataques para usuarios no técnicos

Publicado en: INCIBE

Fecha: 28/10/2020

El Instituto Nacional de Ciberseguridad (INCIBE) pone a disposición de los ciudadanos la 'Guía de ciberataques. Todo lo que debes saber a nivel usuario'. Se trata de una guía que pretende convertirse en documento de referencia para aquellos usuarios de Internet interesados en conocer los tipos de ciberataques a los que se exponen, sin necesidad de tener grandes conocimientos técnicos.

El documento, escrito en un lenguaje sencillo y cercano, recoge las características de todos los ciberataques posibles a los que los ciudadanos pueden enfrentarse con el simple hecho de navegar por la Red. Además, se detalla cómo se realizan estos ataques, el interés que tienen los ciberdelincuentes para ejecutarlos o qué deben hacer los usuarios para estar protegidos específicamente frente a cada uno de ellos y evitar así ser víctimas…

Ver noticia

Ciberataques que matan a las empresas

Publicado en: ElPaís

Fecha: 16/02/2020

Odian contarlo, pero las empresas se están viendo obligadas a admitir lo que pasa en sus sistemas informáticos. Y suelen ser historias espeluznantes. Esta misma semana, Quest Diagnostics, un laboratorio clínico estadounidense que forma parte de las 500 mayores empresas de ese país, ha informado de que los datos de 11,9 millones de pacientes (incluidas tarjetas de crédito y cuentas bancarias) estuvieron ocho meses expuestos por el error de seguridad de un proveedor…

Ver noticia

5. Legislación y normativa

A continuación, se cita la legislación y normativa relacionada con la ciberseguridad:

5.1 Legislación

- Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Ley de Servicios de la Sociedad de la Información (LSSI).
- Ley de Propiedad Intelectual (LPI).

5.2 Normativa

- ISO/IEC 27001 – SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.
- ISO/IEC 2732 – CIBERSEGURIDAD.
- ISO 25012/ISO 25024 – CIBERSEGURIDAD DEL DATO.

6. Bilbiografía

¿Qué es la suplantación de IP?: CLOUDFLARE https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

Abma, J. (2017) HOW TO: SERVER-SIDE REQUEST FORGERY (SSRF): HACKERONE https://www.hackerone.com/blog-How-To-Server-Side-Request-Forgery-SSRF

AENOR. (2011). Gestión de la I+D+i: Sistema de vigilancia tecnológica e inteligencia competitiva. *UNE 166000 EX, UNE 166001 EX, UNE 166002 EX.* Madrid: AENOR.

CETISME, P. (2003). *Inteligencia Económica y Tecnológica. Guía para principiantes y profesionales.* Comunidades Europeas.

Charan, H. (2017).Broken Authentication and Session Management, Part Ⅰ: DZone https://dzone.com/articles/broken-authentication-and-session-management-part

Degoul, P. (1992). *Le pouvoir de l'information avancée face au règne de la complexité.* Annales de Mines.

Diekmann C. & Michaelis J. & Haslbeck M. & Carle G., 'Verified iptables firewall analysis', IEEE Xplore, 2016

Donnelly M., 'Una Introducción a LDAP'

Durumeric Z. & Kasten J. & Bailey M. & Halderman J., 'Analysis of the HTTPS certificate ecosystem', IMC'13, 2013

Escorsa, P. R. (2001). *De la vigilancia tecnológica a la inteligencia competitiva.* Pearson Educación.

Escorsa, Pere, Pilar Lázaro Martínez, Círculo de Innovación en Biotecnología. (2007). Intec: la inteligencia competitiva, factor clave para la toma de decisiones estratégicas en las organizaciones.

Ferguson, P.; Senie, S. "BCP 38" https://tools.ietf.org/html/bcp38, May 2000

Freier A. & Karlton P. & Kocher P., 'The Secure Sockets Layer (SSL) Protocol Version 3.0', 2011

Hassan M, Sultana S., Akter M., Haque R., 'Broken Authentication and Session Management Vulnerability: A Case Study of Web Application', International Journal of Simulation: Systems, Science & Technology, 2018

He S., Moo G., Han S., Whinston A., 'How would Information Disclosure influence organizations' outbound spam volumen? Evidence from a field experiment', Journal of Cybersecurity, Volume 2, Issue 1, 2016

HOW TO: SERVER-SIDE REQUEST FORGERY (SSRF): HackerOne https://www.hackerone.com/blog-How-To-Server-Side-Request-Forgery-SSRF

Information Disclosure Issues and Attacks in Web Applications: NETSPARKER https://www.netsparker.com/blog/web-security/information-disclosure-issues-attacks/

Jaafar F., Nicolescu G., Richard C., 'Systematic Approach for Privilege Escalation Prevention', IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2016

Kagan A. 'Computer security and operating system updates', ScienceDirect, 2003

Keith M. & Shao B. & Steinbart P., 'The usability of passphrases for authentication: An empirical field study', ScienceDirect, 2007

Least Privilege Violation: OWASP https://owasp.org/www-community/vulnerabilities/Least_Privilege_Violation

Man-in-the-Middle (MITM) Attacks: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks

Melnick, J. (2020) What Is Elevation of Privilege?: Netwrix Blog https://blog.netwrix.com/2018/09/05/what-is-privilege-escalation/

O'Gorman G. & McDonald G., 'Ransomware: A Growing Menace', Symantec Security Response

Provos N., Friedl M., Honeyman P., 'Preventing Privilege Escalation', 12th USENIX Security Symposium, 2003

Robert W., 'Naming and Grouping Privileges to Simplify Security Management in Large Databases',Tandem Computers

Server Side Request Forgery: OWASP https://owasp.org/www-community/attacks/Server_Side_Request_Forgery

Server-side request forgery (SSRF): PortSwigger https://portswigger.net/web-security/ssrf

Thomas J. & Galligher G., 'Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware', SSRN, 2018

Villalobos J., 'Vulnerabilidad de sistemas gestores de bases de datos',UNICIENCIA 22 pp. 131-134 , 2008

Wayne C. Summers & Edward Bosworth, 'Password policy: the good, the bad, and the ugly', WISICT'04, 2004

What is a DDoS attack?: CLOUDFLARE https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

What is the Server Side Request Forgery Vulnerability & How to Prevent It?: NETSPARKER https://www.netsparker.com/blog/web-security/server-side-request-forgery-vulnerability-ssrf/

What is the Server Side Request Forgery Vulnerability & How to Prevent It?: NETSPARKER https://www.researchgate.net/publication/241757130_Cross_Site_Scripting_XSS_in_Action

William R. & Kevin E., 'Enterprise Considerations for Ports and Protocols', Institute for Defense Analysis, 2016

Zeilenga K., 'Lightweight Directory Access Protocol: Technical Specification Road Map', 2006