Volumen 3. Número 1. Serie A
ISBN: 978-99939-0-055-9
ISSN: 2708-1141

CyberSecurity

Información & Privacidad

¿Estamos en Ciberguerra?

Las empresas toman la seguridad con la seriedad que merece luego de ser víctimas de un incidente

Archivos de Software Corruptos

La concientización a los usuarios

Ingeniería Social aplicando técnicas de Moving Target

Ataque de phishing vía correo electrónico

Manejo de Malware

Un paso adelante para proteger la reputación de la empresa

DMARC

Un paso adelante para proteger la reputación de la empresa

Guía de negocios básicos

Prevención de fraudes en línea

Información de:

INCIBE GT
Instituto Nacional de Ciberseguridad GT

WOMCY
LATAM Women in Cybersecurity

© Copyright 2020- AUCI

CyberSecurity

Información & Privacidad

Proyecto de:

Con financiamiento de:

ISBN: 978-99939-0-055-9

Publicación de la Asociación Universitaria en Ciencias de la Investigación (AUCI)

Dirección General

AUCI Guatemala

Junta Directiva

2019-2021

Cybersecurity Magazine - Información *y Seguridad*

Universidad Mariano Gálvez de Guatemala
Ing. Daniela de Villatoro
Ing. Criss Velásquez
Ing. Juan Soto
Ing. Armando Monzón

Diseño:
Ing. Darwin Fuentes

Los artículos que aparecen en esta edición no reflejan necesariamente el pensamiento de la Asociación. Se publican bajo la responsabilidad de los autores.

Septiembre – Diciembre 2020

Nota del editor

Con el aumento de riesgos tecnológicos ocasionados por la pandemia del Covid19 vemos la importancia de una concientización a todos los colabores en el uso de las plataformas tecnológicas en nuestras empresas, por lo tanto, la ciberseguridad se convierte en un asunto de interés e importancia para la alta gerencia, en consecuencia, la mejora continua en procesos y/o procedimientos para mitigar riesgos constantes de amenazas, que van desde virus informáticos básicos hasta actividades sofisticadas de ciberdelito y ciber espionaje, así como ciberterrorismo, guerra cibernética entre otros. Esta creciente complejidad de las plataformas tecnológicas digitales en combinación con el aumento de los riesgos globales puede vulnerar valores fundamentales de la sociedad digital como la igualdad, la equidad, la libertad o la privacidad.

En este nuestro tercer volumen vemos reflejadas recomendaciones de los autores quienes han utilizado este canal digital para dar a conocer aspectos de importancia, en este nuestro primer año, hemos logrado mucho, tener a mas de 15 autores exponiendo temas de actualidad, sabemos que nos queda un gran camino por recorrer y lo que empezó como un sueño hoy se ve reflejado en empresas, amigos y autores que nos han dado esa confianza y animo para seguir adelante, en nuestro último volumen del 2020, queremos exhortarles a generar nuevas oportunidades como agentes de cambio en estos tiempos, recalcamos nuestro compromiso con la comunidad tecnológica de Latinoamérica para seguir mejorando y que el 2021 traiga todos éxitos en todos los aspectos de nuestras vidas.

Dani

3 ¿Estamos en Ciber guerra?
Organización Invitada: ISC2 Costa Rica

7 Archivos de Software Corruptos

11 Ingeniería Social aplicando técnicas de Moving Target.

22 Manejo De Malware Destructivo

26 DMARC - Un paso adelante para proteger la reputación de la empresa

33 Guía de negocios básicos - Prevención de fraudes en línea

36 Información de INCIBE GT

38 Información de WOMCY

CyberSecurity
Información & Privacidad

Organización Invitada

ISC2 COSTA RICA

Alejandro Sebiani S.

Presidente de ISC2 Costa Rica Chapter

¿Estamos en Ciber Guerra?

Alejandro Sebiani S.
email: presidencia@isc2crchapter.org
Recibido:22/marzo/2020. Revisado: 17/mayo/2020. Aprobado: 10/julio/2020.
Disponible en internet el 1 de septiembre de 2020

En las guerras tradicionales donde se utilizan bombas y armas, es fácil darse cuenta de que se está en peligro, incluso mucho antes de realmente estarlo y, por lo tanto; se pueden tomar medidas preventivas, persuasivas o correctivas; En la ciberguerra hay ataques todos los días desde hace ya bastante tiempo, sin embargo; es más difícil percibir el peligro y usualmente se piensa que eso sucede en otros países o empresas, pero no en la nuestra.

Lamentablemente, la gran mayoría de las empresas toman la seguridad con la seriedad que merece luego de ser víctimas de un incidente. Es entonces cuando ponen atención a las estadísticas de los ciberataques, a los riesgos existentes y corren a implementar controles por medio de herramientas para mitigar las amenazas.

Existen diferentes formas de pelear una guerra, algunos sin recursos tendrán que luchar con piedras y palos contra tanques, otros serán un pequeño grupo de resistencia escondido y hacinados en una pequeña oficina, habrá quienes tendrán la última tecnología y algunos posiblemente pagarán por su seguridad, porque les resulta más conveniente.

Evidentemente la cantidad de bajas y la probabilidad de ganar una guerra será diferente para cada realidad. Particularmente, me preocupa que las organizaciones implementen herramientas buscando mitigar alguna vulnerabilidad, pero sin tomar en consideración una estrategia de gestión de seguridad de la información y ciberseguridad. Por lo que terminarán con herramientas que posiblemente no harán la diferencia ante un eventual ataque.

Si buscan en Internet, encontrarán muchas estadísticas, ¿cuáles son los vectores de ataque más utilizados?, ¿cuál es el origen de los ataques, la motivación, el monto, el tipo de empresa?, etc. Yo solamente quisiera darles un dato, publicado precisamente en uno de los tantos informes que se generan al año y que quienes no han sido víctimas posiblemente los leen como un dato de algo que está muy lejano a sus empresas: Solamente en Estados Unidos, el FBI en su reporte anual de crimen por Internet, estimó las pérdidas del 2019 en 3.5 billones de dólares.

Si buscan quienes son las víctimas, se identificarán empresas de servicios, bancos, aseguradoras, telefónicas, escuelas, universidades, hospitales, empresas de Gobierno, incluso militares, empresas grandes, medianas y pequeñas. Una de las últimas víctimas fue la fábrica de autos Honda, quienes tuvieron que detener su producción a nivel mundial, con el evidente impacto económico producido no solo por la paralización de la empresa, sino por las acciones que requerirán para retomar su operación.

En un mundo en donde los servicios ofrecidos por las empresas están basados en tecnología y en la información, un incidente de seguridad podría tener un alto impacto económico y de imagen. En aquellas empresas como las financieras, que se basan en la confianza de los clientes, podría ser catastrófico y fácilmente llevar a una empresa a la quiebra.

Lo cierto es que, no existe seguridad absoluta, esto es una máxima que las empresas deben tener siempre presente y es indispensable que entiendan que la seguridad de la información no es un asunto

técnico, no se trata de hardware o software, la seguridad de la información y ciberseguridad es un asunto estratégico.

¿Cómo hago para que mi empresa sea segura?

Debemos tener presente que la seguridad no es una actividad, es un proceso continuo, que tal y como lo indica ISO27001 se basa en el ciclo Planear-Hacer-Revisar-Corregir (PDCA por sus siglas en ingles) y por tanto, no basta con implementar controles o herramientas, es indispensablemente realizar una adecuada gestión de la seguridad de la información.

Los controles de seguridad por su parte deben originarse en una adecuada identificación de riesgos, el no hacerlo, tiene el gran riesgo de omitir riesgos. El trabajo conjunto de las áreas de riesgo y de seguridad es indispensable, para garantizarnos un enfoque y una atención integral. Debemos apegarnos a un estándar o marco de referencia, tal como ISO27001 o el Modelo de Ciberseguridad emitido por Instituto Nacional de Estándares y Tecnología del Ministerio de Comercio de Estados Unidos (NIST).

"La seguridad de la información y ciberseguridad es un asunto estratégico"

Es usual, que muchas áreas de tecnología no vean con buenos ojos el trabajo de las áreas de Riesgo y de Seguridad de la información, porque consideran que de forma ingrata evidencian los errores en su gestión, sin entender la importancia para el negocio de tener claridad sobre cuáles son sus riesgos y cuál es su verdadero nivel de seguridad. Solamente teniendo presente cuales son las brechas, éstas podrán ser atendidas de acuerdo con las prioridades del negocio. Si su empresa piensa de esa forma muy posiblemente pronto será una víctima más.

Asegurar una empresa es trabajo de todos los miembros de la empresa, algunos con mayor o menor participación, pero todos deben al menos aplicar en su puesto de trabajo las medidas de seguridad que han sido definidas por el área de Seguridad de la información en relación con el plan de Ciberseguridad que planteen.

Por desgracia los que más frecuentemente obvian los controles de seguridad son quienes más deberían aplicarlos, y me refiero al personal de tecnología, que muchas veces en su afán de servicio busca erróneamente como obviar los controles de seguridad e incluso áreas como soporte técnico facilitan a usuarios "amigos" las herramientas para vulnerar los controles, como por ejemplo para poder navegar "libremente" o para instalar software. Por otro lado, es usual que se generen excepciones para algunos grupos, por ejemplo: nadie puede instalar software en sus equipos, pero las jefaturas sí.

Es imposible para una sola persona o un grupo a cargo de la Seguridad de la información y Ciberseguridad, poder asegurar su empresa, porque la seguridad tiene que ver prácticamente con todos los procesos, servicios y actividades de la empresa. Es por eso por lo que la disciplina en la adopción y aplicación de los controles de seguridad debe ser estricta.

Posiblemente en estos tiempos, nadie dejará las llaves pegadas en la puerta de la entrada, porque existe conciencia del riesgo que eso implica, precisamente con ese mismo nivel de consciencia es que cada persona debe entender y aplicar los controles de seguridad, porque de lo contrario, es aquí en donde las herramientas por más sofisticadas que sean perderán su efectividad y valor.

Si queremos ganar esta guerra, debemos conocer nuestros riesgos, nuestro nivel de Ciberseguridad, tener una estrategia clara orientada a garantizar la disponibilidad de nuestros servicios y la continuidad de nuestro negocio y para esto, el área de Seguridad necesita tener el empoderamiento y el respaldo requerido de parte de la Organización.

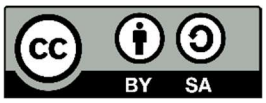
Sobre el autor:

Profesional experimentado y líder dedicado de TI, enfocado en estrategia empresarial con excelente conocimiento técnico. Capaz de desarrollar estrategias y planes con una visión holística basada en procesos, personas y tecnología orientados a mejorar la experiencia del usuario, generar valor para las partes y optimizar el uso de los recursos.

Estudios en tecnología y administración de empresas, me permiten comprender las necesidades del negocio, identificar problemas o limitaciones y liderar la definición e implementación de soluciones innovadoras en entornos de alta complejidad; Teniendo en cuenta los aspectos de seguridad y riesgo de la información, pero convirtiendo los controles en habilitadores comerciales.

Habilidades

• Visión empresarial, teniendo en cuenta que la tecnología es el medio para alcanzar los objetivos empresariales y no el fin. Definición, ejecución y seguimiento de planes estratégicos y tácticos. Análisis, rediseño, optimización e implementación de procesos para mejorar la operación. Analítico, acostumbrado a la toma de decisiones en función del riesgo y con un adecuado equilibrio costo-beneficio. Conocimiento y experiencia en la definición e implementación de metodologías, políticas y procedimientos. Conocimiento de las leyes y regulaciones aplicables al gobierno, el sector financiero y el sector tecnológico. Administración de recursos humanos, liderazgo de equipos, trabajo bajo presión y 24x7 horas. Enfoque práctico y orientado a resultados. Conocimiento y experiencia en Gestión de Proyectos. Conocimiento y experiencia en las principales áreas de la tecnología, tales como Monitoreo, operación, programación, bases de datos, soporte técnico, seguridad, riesgo y telecomunicaciones. Responsable, honesto, motivador, humilde, persuasivo, enfocado en objetivos. Especializado y certificado internacionalmente en Seguridad y Riesgo de la Información. Empático, negociador, capaz de generar alternativas y encontrar la mejor solución con un enfoque win-win. Generador organizado, creativo y de iniciativa. Experiencia en la implementación y alineación a estándares internacionales y marcos de referencia como ISO, Cobit, PCI / DSS. Conocimiento de la normativa emitida por CONASSIF para el sector financiero. Conocimiento de la Ley Orgánica del Banco Central de Costa Rica. Conocimiento de la Ley General de Administración Pública, Ley de Contratación Administrativa, Ley General de Control Interno, Ley contra la Corrupción y Enriquecimiento Ilícito y otras leyes aplicables al Gobierno y sector financiero.



CyberSecurity
Información & Privacidad

Artículos

CyberSecurity
Información & Privacidad

Archivos de software Corruptos, una de las amenazas más importantes cuando se trata de concientizar a los usuarios.

Corrupt software files, one of the most important threats when it comes to raising user awareness

Xavier Aarón Gribble Arredondo
email: xgribble@gmail.com
Recibido:6/marzo/2020. Revisado: 12/mayo/2020. Aprobado: 10/julio/2020.
Disponible en internet el 1 de septiembre de 2020

Resumen: Las medidas de ciberseguridad no son una solución perfecta y no garantizan la protección e integridad de su información cuando se enfrentan a archivos corruptos. Esto se debe a que dichos archivos pueden tener muchos formatos y extensiones diferentes y pueden apuntar a una amplia variedad de software. Además de eso, los archivos corruptos se pueden distribuir a través de sitios web, correo electrónico o redes internas, lo que convierte a esta amenaza en una de las amenazas más importantes cuando se trata de concientizar a los usuarios. A medida que las amenazas evolucionan para volverse más sofisticadas, las empresas de todas las industrias han comenzado a tomar medidas para mejorar sus esfuerzos para mantener sus datos seguros. Incluso las pequeñas empresas que no se habrían molestado con la ciberseguridad hace unos años. Esto se debe a que ahora se pueden encontrar amenazas en una amplia variedad de fuentes, no solo en las fuentes que más se esperan, como archivos adjuntos en línea o por correo electrónico. Los atacantes también pueden explotar vulnerabilidades en software de uso común y modificar o inyectar su propio código malicioso.

Palabras Claves: covid-19, robo de información, archivos corruptos, dispositivos, amenaza.

Abstract: Cybersecurity measures are not a perfect solution and do not guarantee the protection and integrity of your information when faced with corrupt files. This is because such files can have many different formats and extensions and can point to a wide variety of software. On top of that, corrupted files can be distributed via websites, email, or internal networks, making this threat one of the most important threats when it comes to raising users' awareness. As threats evolve to become more sophisticated, companies in all industries have begun to take steps to improve their efforts to keep their data safe. Even small businesses that wouldn't have bothered with cybersecurity a few years ago. This is because threats can now be found from a wide variety of sources, not just the most anticipated sources, such as email or online attachments. Attackers can also exploit vulnerabilities in commonly used software and modify or inject their own malicious code.

Desarrollo:

No son solo las empresas o los dueños de negocios los que necesitan protección contra los atacantes, los gobiernos tambien han implementado nuevas regulaciones a lo largo de los años para garantizar la privacidad de la información personal y la información financiera de las empresas. Los gobiernos también han estudiado la posibilidad de que el software propietario pueda incluir fallas o características maliciosas que podrían generar vulnerabilidades. Microsoft estableció el Programa de Seguridad del Gobierno (GSP por sus

siglas en ingles) para que los gobiernos pudieran analizar su fuente (Gao, Ken. "China to view Windows code". CNET.).

La ciberseguridad está ayudando a mantener a los negocios en funcionamiento e incluso ayuda a mantener la forma de vida de las personas. Debido a que las actividades cotidianas de millones de personas en todo el mundo dependen del uso de la tecnología y la información que se almacena y distribuye a través del uso de la misma, existe una gran necesidad de proteger la integridad de los activos tecnológicos contra las amenazas de ciberseguridad. Una seguridad cibernética deficiente podría presentar muchos riesgos en diferentes niveles de gravedad; podría resultar en el robo de información, la eliminación de sistemas completos o el uso de nuestros dispositivos para atacar a otros dispositivos, entre muchas otras posibilidades.

Como se mencionó anteriormente, las amenazas de ciberseguridad han evolucionado a un ritmo acelerado. Podría decirse que la primera versión de un virus informático se creó en 1971. El primer y pequeño numero de personas que usaron ARPANET en ese entonces, comenzaron a ver el mensaje: "I'm the creeper, catch me if you can.". exhibido en su pantalla. Este virus era un gusano, se replicaba y llegaba a otras computadoras y sistemas, pero todo lo que hacía era mostrar un mensaje. Era, en cierto modo, solo un graffiti digital.

Después de esto, los primeros virus famosos comenzaron como archivos aparentemente normales que aprovecharon las vulnerabilidades en los sistemas operativos de las computadoras. Debido a esto, hubo un aumento en los productos de seguridad que analizarían todos los archivos en un sistema y los compararían con "firmas" conocidas, lo que significaba buscar cadenas de texto que se encontraban previamente en amenazas conocidas.

Aunque los archivos corruptos fueron parte de las primeras etapas de las amenazas de ciberseguridad, todavía son una amenaza importante hoy en día. Los atacantes siguen buscando y encontrando vulnerabilidades en los principales productos de software y aprovechándolos para crear sus propios archivos maliciosos que pueden infectar o abrir puertas traseras en los sistemas.

Solo para enumerar algunas posibilidades, este archivo "malo" podría comenzar a hacer que la computadora consuma más ancho de banda o más memoria y esto resultaría en una disminución de la capacidad de la PC para procesar información, para el usuario esto podría no ser visible, pero lo que el usuario sentirá que la PC es más lenta o no reacciona tan rápido como antes; este archivo "malo" también podría estar alterando, agregando o eliminando archivos importantes en la computadora con el propósito de volver a hacer que se bloquee o, lo que es peor, obtener acceso no solo para robar información personal sino incluso para usarla para dañar a otros, empeorando las consecuencias exponencialmente.

La corrupción intencional de archivos ahora es algo tan común, tan normal, tan evidente que incluso puede encontrar sitios web que le ofrecen la posibilidad de corromper un archivo. Algunos ejemplos de estos sitios web son www.corruptmyfile.com, corrupt-a-file.net en las cuales, básicamente con solo un par de clics obtienes el archivo que querías que se corrompiera.

Al descargar archivos de un sitio web, no siempre sabremos que nuestro archivo descargado está dañado o no solo al mirar el tipo de archivo. Hace años era más común escuchar que había un tipo específico de archivos para tener en cuenta, por ejemplo, un tipo de archivo ejecutable, si deseábamos descargar un archivo .pdf pero el sitio web descargaba un archivo .exe, sabíamos que no teníamos que abrirlo/ejecutarlo, pero los atacantes han evolucionado a medida que la tecnología lo ha hecho, ahora pueden corromper cualquier tipo de archivo, insertando código malicioso en ellos.

Los atacantes aprovechan las necesidades de las personas, sabiendo que tienen la urgencia de resolver sus problemas. Los atacantes también pueden aprovechar las noticias, situaciones e intereses actuales. Por ejemplo, un sitio web que brinda información sobre el Covid-19, que ofrece un enlace para descargar un documento con instrucciones para prevenirlo. Con la actual paranoia y preocupación que esto está causando en la sociedad, la gente está tratando de obtener tanta información como sea posible, y los atacantes que se aprovechan de eso, podrían hacer daño fácilmente.

Las amenazas de archivos corruptos también pueden apuntar a versiones específicas de cualquier software dado, La mayoría de los principales proveedores de software lanzan constantemente nuevas versiones de sus productos para realizar mejoras constantes, corregir errores y, lo que es más importante, corregir vulnerabilidades de seguridad que han demostrado ser explotables o que han sido detectadas al realizar sus propias pruebas. Por lo general, es por lo primero. Los atacantes encuentran vulnerabilidades que pueden explotarse en una versión específica de un software específico y el fabricante del software actúa en consecuencia para lanzar una nueva versión. Debido a esto, los usuarios deben actualizar todo el software constantemente para garantizar que sus dispositivos estén actualizados en lo que respecta a la ciberseguridad.

Debido a que los tipos de archivos comunes pueden estar corruptos, algunos dispositivos de seguridad diferentes pueden no reconocer la amenaza que representan los archivos dañados. Es común que usuarios inconscientes descarguen archivos de un sitio web o de correos electrónicos entrantes, por lo general, si un usuario reconoce el tipo o la extensión del archivo, no lo pensará dos veces antes de abrir o ejecutar un archivo. Algunos dispositivos o software de seguridad de alta gama probablemente analizarán dichos archivos y reconocerán amenazas; sin embargo, estos dispositivos generalmente funcionan comparando firmas de archivos con conjuntos de datos de amenazas comunes y podrían no reconocer una amenaza encontrada en un tipo de archivo común.

Muchas amenazas de ciberseguridad se disfrazan como herramientas de ciberseguridad y, por lo general, requerirán una acción del usuario para infectar un dispositivo. Cuando nos referimos a la rápida evolución y mejora de diferentes tipos de amenazas, debemos reconocer que la falta de conocimiento o conciencia de los usuarios juega un papel importante en la efectividad de una amenaza.

Referencias bibliográficas

Jessica (2018). What is a Corrupted File? Cybrary. https://www.cybrary.it/blog/2018/06/what-is-a-corrupted-file/

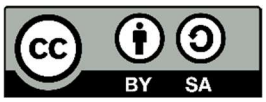
CISA (2019). Security Tip (ST04-001). https://www.us-cert.gov/ncas/tips/ST04-001

Mindi McDowell (2019). Understanding Hidden Threats: Corrupted Software File. CISA. https://www.us-cert.gov/ncas/tips/ST06-006

John Walker (2006). "Corrupted Downloads" What Is to Be Done? Fourmilab.https://www.fourmilab.ch/documents/corrupted_downloads/eartbleed,

Sobre el autor:

Desarrollador con 7 años de experiencia trabajando en ABAP, C#, y Apex (Salesforce). Actualmente labora como full stack Developer para la empresa estadounidense Torrent Consulting. Cuenta con las certificaciones Salesforce Admin, Platform App Builder y Platform Developer I, otorgadas por Salesforce.



CyberSecurity
Información & Privacidad

Ingeniería Social aplicando técnicas de Moving Target por medio de ataque de phishing vía correo electrónico.

Social Engineering applying Moving Target techniques through phishing attack via email

Roberto Lemaître Picado

La presente investigación surge como proyecto final del curso Diversificación en Seguridad Computacional PF-3899, de la Maestría Profesional en Computación de la Universidad de Costa Rica, impartido por la profesora Elena Gabriela Barrantes Sliesarieva, Ph.D.
El proyecto consistió en aplicar un ataque, con diversificación.
email: rolemaitre@abogados.or.cr
Recibido:22/marzo/2020. Revisado: 10/mayo/2020. Aprobado: 12/julio//2020.
Disponible en internet el 1 de septiembre de 2020

Resumen: Cada día son más comunes los ataques informáticos basados en la ingeniería social. Estos ataques aprovechan la confianza de los usuarios para tener acceso a información confidencial. Entre ellos, se destaca el phishing, el cual consiste en obtener información confidencial utilizando la ingeniería social mediante el envío de mensajes fraudulentos para engañar a la víctima y forzarla a tomar una decisión rápidamente. Debido a su peligrosidad, esta investigación buscó realizar un ataque de ingeniería social por medio phishing de correo electrónico de manera tradicional (sin diversificar); y otro ataque con diversidad, con el fin de determinar la efectividad de cada uno y cuál le genera más confianza al grupo de personas estudiadas de una institución pública. Además, se pretendió crear conciencia digital para que se conozca este tipo de ataque y los riesgos que implica, de esta forma se mejorará la ciberseguridad de la institución.

Palabras Claves:Ciberseguridad, inteligencia artificial, amenaza, ataques, ciber delincuentes.

Abstract: Every day, computer attacks based on social engineering are more common. These attacks take advantage of users' trust to access confidential information. Among them, phishing stands out, which consists of obtaining confidential information using social engineering by sending fraudulent messages to deceive the victim and force her to make a decision quickly. Due to its dangerous nature, this investigation sought to carry out a social engineering attack by means of email phishing in the traditional way (without diversifying); and another attack with diversity, in order to determine the effectiveness of each and which generates more confidence in the group of people studied in a public institution. In addition, it was intended to create digital awareness so that this type of attack and the risks involved are known, thus improving the institution's cybersecurity.

Desarrollo:

Lo frecuente, en este tipo de ejercicios, es realizar defensas o ataques entre máquinas, pero al final, el eslabón más débil de la seguridad y ciberseguridad es la persona. En ese sentido, resulta de mucho interés estudiar el fenómeno de ataques con diversidad versus los tradicionales, en materia de ingeniería social, y específicamente, en temas de ataques con *phishing* vía correo electrónico, pues este es, actualmente, uno de los riesgos que más genera efectividad al *cibercrimen*. Al respecto, las estadísticas del primer trimestre de 2016 de

Kaspersky señalan que: *"Los correos electrónicos maliciosos han crecido significativamente en los últimos meses, según estadísticas de Kaspersky, los productos de la empresa de seguridad han detenido casi 23 millones de intentos de infección a sus usuarios a través de correos con archivos maliciosos adjuntos, esta cifra ha sido únicamente en el mes de marzo de 2016, justo el doble de lo reportado en febrero de este mismo año, lo que indica que a los cibercriminales les sale muy rentable y seguramente esta cifra aumente."* [1]

Resulta importante para comprender el desarrollo de la investigación debemos vislumbrar dos conceptos importantes:

- **La Ingeniería Social,** es *el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Estas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo.*[2]
- **El *Phishing*,** consiste *en el envío de mensajes (anzuelos) a una o varias personas, recurriendo a la suplantación de la identidad de una empresa o entidad pública con el objetivo de persuadir a la futura víctima para revelar sus datos personales o financieros que involucran nombres de usuario y contraseñas. Una vez obtenida esta información es utilizada con fines maliciosos para realizar acciones como transferencias de fondos a cuentas bancarias y compras con tarjetas de crédito entre otras acciones delictivas que afectan económicamente a la víctima.*[3]

Asimismo, el ataque real se realizó en una institución del sector público, con el fin de generar conciencia sobre el riesgo del *phishing* y desarrollar una mejor cultura digital ante este tipo de acciones en el Estado

El trabajo buscó responder y aportar de manera introductoria a la investigación de campo realizada con base en el siguiente problema: "¿qué tipo de ataque de *phishing* por medio de correo electrónico es más efectivo: con diversidad o sin diversidad en una institución del estado costarricense?"

Asimismo, se esperó determinar cuál ataque de *phishing* por correo electrónico fue más efectivo, si el realizado con diversidad o el efectuado sin diversidad y poder identificar la efectividad del ataque de *phishing* en una institución del estado costarricense.

---

[1] Sitio Web Redes Zone http://www.redeszone.net/2016/05/29/aumenta-spam-malicioso-primer-trimestre-del-2016-segun-informe-kaspersky/#sthash.7oCRXgkR.dpuf

[2] Revista Seguridad UNAM 10: Ingeniería Social: Corrompiendo la mente humana
http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

[3] Revista de Seguridad UNAM 02: Pescando Información Phishing
http://revista.seguridad.unam.mx/numero-02/pescando-informaci%C3%B3n-phishing

La solución aplicada consistió en elaborar un ataque de diversidad por medio de la técnica de *phishing,* utilizando el medio tecnológico del correo electrónico, aprovechando ingeniería social para pedir información del usuario. La institución donde se realizó el ejercicio de ataque fue del sector público; la cual cuenta con cincuenta y cuatro funcionarios. Cada uno de ellos tiene asignado un correo electrónico institucional con la siguiente estructura: nombre.apellido@institucion.go.cr, el cual es un dominio contratado a la empresa Google por medio del servicio *gmail*. Veinte funcionarios fueron tomados como muestra, a ellos se les solicitó el consentimiento para participar en el proyecto. Los veinte funcionarios notificados se dividieron en dos grupos; al primer grupo de diez de ellos se le envió un ataque normal, sin diversificar; y al segundo grupo de diez personas se le envió un ataque diversificado.

De manera precisa, a los primeros diez se les envió el ataque normal de *phishing* sin diversificar en tres ocasiones. El ataque se efectuó de la siguiente forma: se envió en el primer ataque un correo a cada persona seleccionada. Se esperó dos días para enviar una segunda "ola" de ataque, en la cual se enviaron dos correos electrónicos; posteriormente se esperó tres días más para realizar la tercera "ola" de ataque. En esta última se enviaron tres correos electrónicos. En el caso del ataque diversificado se varió ligeramente su contenido (se diversificó); de igual forma se envió el correo electrónico en la misma cantidad y secuencia de días y también se personalizó con el nombre de la persona. La idea fue que el contenido del correo solicitara una respuesta al mismo, de esta forma, el hecho de responder el correo convertía el ataque en exitoso, independientemente de si respondía lo solicitado o no. A todos los funcionarios se les solicitó el consentimiento informado para participar en el ejercicio.

Cada correo de respuesta de cada "ola" de ataque se contabilizó para generar una estadística de cada ataque, con diversidad y sin diversidad, y determinar el éxito de cada uno. De esta forma, se comparó el éxito del ataque de diversidad versus el no diversificado. En el caso del diversificado, el correo de *phishing* varió ligeramente en los párrafos que lo conforman. El contenido del mensaje se estructuró de la siguiente forma:

- Logo: se creó un logo relacionado con la temática de la institución.
- Tema del correo: cambios en la política de seguridad de la entidad.
- Contenido: se crearon varios párrafos referidos al tema del cambio de la política de la seguridad de la entidad, haciendo que variara cada correo en pequeños detalles.

Párrafos de contenido del mensaje:

Estimados funcionarios y funcionarias de XXXX:

Párrafo versión 1: *"Por este medio deseamos informales que en pro de mejorar la seguridad tecnológica de nuestra institución estamos recabando datos de cada funcionario por lo que agradecemos nos responda con la siguiente información:"*

Párrafo versión 2: "*Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben cumplir todos los funcionarios que trabajan para la institución, por lo que es obligatorio brindarnos la siguiente información:"*

Párrafo versión 3: "*El XXXX identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que la institución establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que esta sea manejada, procesada, transportada o almacenada, es por esta razón que le solicitamos la siguiente información:"*

Párrafo estándar para ataque sin diversidad: *"Es necesario que nos envíe, vía correo electrónico, los siguientes datos para verificar y cumplir aspectos relacionados con las Políticas de Seguridad de la Información de la Institución:"*

- *Nombre Completo: _____*
- *Cédula: _____*
- *Tipo de computadora: Laptop____ PC____*
- *Sistema Operativo: Windows 7___ Windows 8__ Windows 10__ Mac___*

Agradecemos de antemano su ayuda y colaboración para mejorar nuestra institución

Gracias

Nombre Persona a Cargo del Soporte
Logo
Unidad de Servicios Tecnológicos
Teléfono

El envío de los correos se realizó por medio de un correo falso, creado en *gmail*, el cual se denominó serviciostecnologicos@xxxx.com. Luego de creado se utilizó la herramienta SET para el envío. Al abrir la herramienta SET se escogió la función *Social-Engineering Attacks*; dentro de este menú se escogió la opción *Mass Mailer Attack.* Ahí aparecieron dos tipos de opciones de envío, la primera indicó que se enviaría un email a una sola persona, y la segunda, que se enviaría un correo a diferentes personas. Para este proyecto, se escogió la segunda opción.

En esta etapa se había creado un archivo *.txt* con la lista de correos a los que se les envió el ataque. Las direcciones electrónicas de los funcionarios son conocidas por el investigador. Luego, se seleccionó el fichero de texto *.txt* donde estaban los emails para enviar el correo; seguidamente se indicó si el correo del remitente es de *gmail* o no, en este caso sí se utilizó el correo creado de *gmail.* Posteriormente, se solicitó indicar si el mensaje era de importancia o no, aquí se señaló la opción de *alta prioridad;* en *Asunto* se anotó: *Urgente Política de Seguridad de la Información XXXX*. También, se seleccionó el formato del correo, en este caso se utilizó *Html*; se presiona Ctrl + C y se envía.

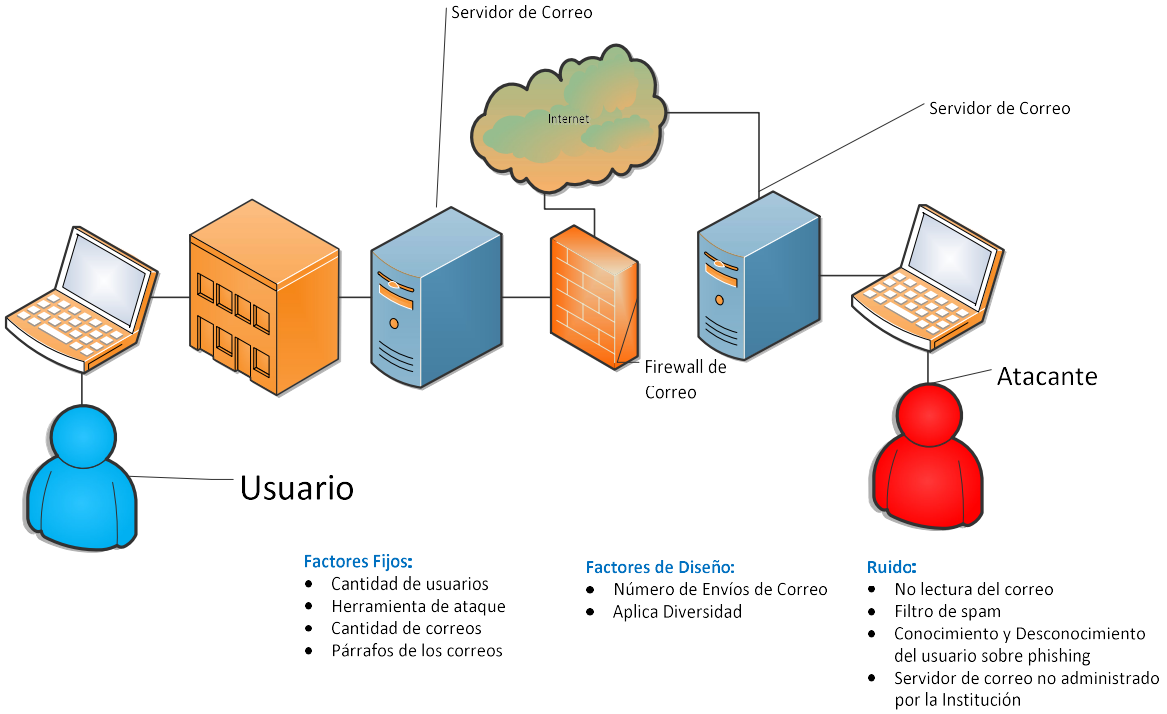


Ilustración 1 Diseño del proyecto
Fuente: Elaboración propia

Las defensas con que contaba la institución podemos establecerlas de la siguiente forma:

Defensa Técnica:

- El filtrado que puede realizar el correo de dominio de la institución. El correo institucional lo provee la empresa Gmail, por lo que presenta un filtrado de correo *SPAM* o sospechoso,
- Spam y correos sospechosos: *Gmail cuenta con un sistema automatizado que ayuda a detectar spam y mensajes sospechosos a través de la identificación de virus, la localización de patrones en los mensajes y el análisis de lo que los usuarios de Gmail como tú suelen marcar como spam.*[4] Esto podía generar que el correo no ingresara a la bandeja de entrada de los usuarios

Defensa Humana:

- El usuario puede determinar que el correo no es oficial, depende de si ha recibido o no información para sospechar de este tipo de correos, o del hecho de no acostumbrar a brindar información por estos medios. Este aspecto podía generar que no se contestara a los correos.

[4] Fuente: Soporte Gmail https://support.google.com/mail/answer/1366858?hl=es

Para el caso de las *variables de respuesta*, estas fueron:

a. Nombre: respuesta del correo por persona.

b. Descripción: respuesta por usuario de cada ataque de *phishing* enviado, con diversidad y sin diversidad, independientemente de si se brindó la información solicitada por parte del usuario. Se creó una tabla para comparar respuestas de usuario en cada "ola" de ataque.

c. Unidades (si tiene): respuesta por persona, 0 para no respondió, 1 para sí.

Factores de diseño

Los factores de diseño fueron:

a) Factor de Diseño 1

a. Nombre: Número de envíos

b. Descripción: Cantidad de correos enviados por cada ataque, tanto del *phishing* tradicional como diversificado.

c. Unidades: número de correos por ataque.

d. Niveles y justificación: Se envió un correo diversificado y sin diversificar en el primer nivel de ataque. En el segundo nivel se esperó dos días para enviar una segunda "ola" de ataque, en la cual se enviaron dos correos con el contenido de correo diversificado y el mismo correo sin diversificar. En el tercer nivel se esperaron tres días para realizar la tercera "ola" de ataque con el contenido del correo diversificado; en esta última se enviaron tres correos y la misma cantidad sin diversificar.

Se comparó cada nivel de ataque de diversidad y la respuesta de cada persona versus el ataque sin diversidad y la respuesta de cada persona, según el grupo atacado.

b) Factor de Diseño 2

a. Nombre: Aplica diversidad.

b. Descripción: Variantes del correo de ataque con cada párrafo ligeramente distinto para cada usuario enviado con ataque diversidad.

c. Unidades: No aplica.

d. Niveles y justificación: Se crearon tres niveles. Cada uno tuvo un párrafo distinto con un sentido diferente de solicitud: uno en tono amistoso, otro a manera de orden, y otro neutral. Así se podría comparar más adelante con el ataque sin diversidad.

Factores Fijos

Se desarrolló el siguiente factor fijo: Cantidad de usuarios: La cantidad de usuarios a quienes se les envió el correo de phishing fue la misma durante todo el proceso, y fue un grupo "cautivo" de la institución. Herramienta técnica SET (Social-Engineering Toolkit)[5]

Se utilizó la herramienta *SET* (*Social-Engineering Toolkit*), *SET* es una *suite* dedicada a la ingeniería social, permite automatizar tareas que van desde el envío de SMS (mensajes de texto) falsos, con los que podemos suplantar el número telefónico que envía el mensaje, a clonar cualquier página web y poner en marcha un servidor para hacer *phishing*.

El kit de herramientas *SET* está especialmente diseñado para realizar ataques avanzados contra el elemento humano. Es uno de los equipos estándar para las auditorías de seguridad.

Imagen 1 Pantalla principal de la herramienta SET

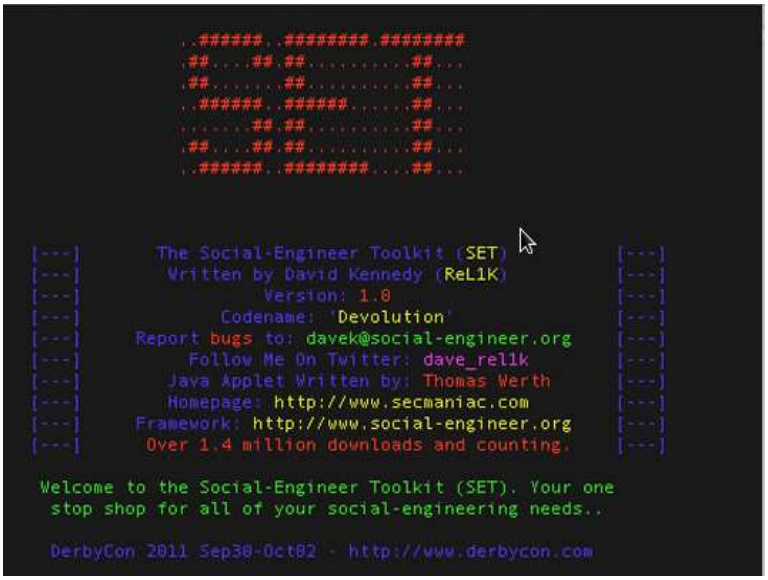


Ilustración 2 Pantalla Principal de la herramienta SET

Fuente: Pantalla de SET, tomado de http://www.blog.xentech.cl/wp-content/uploads/2016/01/seleccic3b3n_375-298x248.png

Cantidad de correos: Se envió un correo en la primera "ola" de ataque junto al párrafo 1, luego de dos días, en la segunda "ola" de ataque dos correos con el párrafo 2 y luego de tres días tres correos de ataque con el párrafo 3.

Párrafos de los correos: Se envió cada "ola" de correos con un tipo de párrafo distinto. Para el ataque diversificado cada uno respondió a un conjunto de usuarios específicos; y para el ataque sin diversidad se creó un párrafo estándar de ataque *phishing*.

[5] Para más información Introducción a Social-Engineering Toolkit (SET)
http://www.hackplayers.com/2012/10/social-engineering-toolkit-set.html

Factores de ruido: En el caso de los factores de ruido consideré los siguientes:

1. La posibilidad de que simplemente las personas no leyeran el correo por las diferentes labores que realizan, no le prestaran importancia y, en consecuencia, no respondieran el correo.

2. Filtro del correo el cual enviara el correo de *phishing* a *SPAM*. A pesar de ser un factor de defensa, es un factor de ruido también, pues al provocar que los correos no sean leídos por el usuario, ni siquiera existe la oportunidad de responder el *phishing.*

3. El conocimiento o desconocimiento que tenga el usuario sobre temas de seguridad relacionados con *phishing*.

4. El servidor de correos, el cual no es administrado por la institución, es contratado a la empresa *Gmail*.

5. El solicitar el consentimiento informado, lo cual ponía en alerta a la población estudiada, podría esperar ser atacada.

Metodología del ataque: El proceso desarrollado se describe a continuación:

1. Se elaboraron los correos electrónicos para *phishing* con base en el contexto de la institución.

2. Se creó un correo falso, muy parecido al formato institucional, para enviar los correos de *phishing*.

3. Se obtuvo la lista de correos de la institución de las personas seleccionadas.

4. Se creó un archivo de extensión *.txt* con la cantidad de emails que se deseaba enviar.

5. Se ejecutó *SET*, *Set console*, en el cual se siguió el proceso para el envío de este tipo de ataque.

6. Se seleccionó la opción para enviar muchas direcciones, se solicitó la ruta en la cual se tiene el *.txt* con los correos.

7. Se solicitó la cuenta de correo electrónico para que enviara los correos electrónicos masivos, se realizó con la cuenta falsa.

8. Se seleccionó, en la herramienta de *SET*, el ataque masivo vía correo electrónico, el envío de correo masivo y adjunto del dato tipo *FileFormat.*

9. Se verificaron los datos generados, los cuales fueron ofrecidos por los usuarios que cayeron en el *phishing* en las cuentas de registro de usuarios.

10. Recolección de los datos. Se llevó a cabo una estadística digital de respuestas a los correos por cada "ola" de ataque, para lo cual se utilizaron tablas.

11. Análisis de resultados. Se estudiaron las cantidades de respuestas realizadas por cada "ola" para describir lo exitoso, o no, de cada ataque y de cada variante del correo.

12. Presentación de resultados.

Resultados

El resultado fue muy interesante para los fines de la investigación, y, por otro lado, muy alarmante para el contexto de la institución. En las tablas 1 y 2, se observan los resultados de cada "ola" de ataque por cada ataque diversificado y sin diversificar.

En el caso de los ataques sin diversificación, estos presentaron una respuesta alta, tanto en la primera "ola" de ataque, como en la segunda, lo que representó la respuesta más positiva del ataque. Es importante indicar que, ejecutadas las tres olas de ataque, solamente dos personas no respondieron el correo de *phishing* sin diversificar. Además, es interesante mencionar que una persona detectó el ataque.

Tabla 1 Resultado ataque *phishing* sin diversificar

	Sin diversificar Respondieron	Sin diversificar No respondieron	Sin diversificar Detectaron
"Ola" de ataque 1	1,1,1,1		
"Ola" de ataque 2	1,1,1		1
"Ola" de ataque 3		1,1	

Fuente: Elaboración propia con base en los resultados del ataque de *phishing* por correo realizado.

Para el caso de los ataques con diversificación, se refleja una menor respuesta por parte de los usuarios. En comparación con el ataque no diversificado, en la primera "ola" solamente respondieron tres personas. De igual forma, es importante indicar que en la categoría de "no respondieron" en el ataque diversificado se refleja que, realizadas las tres "olas" de ataque, los usuarios seguían sin responder. Además, un dato significativo es que en este tipo de ataque se detectó mucho más que el correo era un intento de *phishing* (tres personas lo detectaron); mientas que en el ataque sin diversificar solamente una persona lo detectó. En comparación, fue más efectivo el ataque sin diversificar que el ataque diversificado.

Tabla 2 Resultado ataque *phishing* diversificado

Olas de Ataque	Diversificado Respondieron	Diversificado No respondieron	Diversificado Detectaron
"Ola" de ataque 1	1,1,1		1,1
"Ola" de ataque 2			
"Ola" de ataque 3		1,1,1,1	1

Fuente: Elaboración propia con base en los resultados del ataque de *phishing* por correo realizado.

De manera general, los resultados, señalan que, de los veinte participantes del ataque, diez personas sí respondieron el ataque, seis no respondieron y cuatro detectaron el ataque falso. Esto demuestra que existió un **50% de respuesta positiva**, lo cual es un dato preocupante y una cifra muy alta para una institución en la que todos sus funcionarios son profesionales muchos relacionados día a día con temas tecnológicos.

Asimismo, en términos generales, los usuarios que respondieron el correo brindaron la siguiente información de índole privada de cada equipo que las personas utilizaban. En este sentido, logré determinar que Windows 7 y Windows 10 son los más utilizados. El aporte de este dato es peligroso pues, eventualmente, podría prepararse un ataque con esta información. Una estrategia de ataque consideraría este tipo de dispositivo como el predominante en la institución.

También, se puede apreciar que la mayor cantidad de equipos utilizados en la Institución son computadoras portátiles, con base en la información brindada por las personas que cayeron en el *phishing*. Este dato también brinda información inicial para que un atacante planee su estrategia a seguir.

Así mismo, en la primera "ola" de ataque se dio mayor contestación; mientras que en ninguna de las otras dos "olas" de ataque hubo respuestas. Esto significa que la insistencia de respuesta no produjo cambios en quienes no habían respondido en la primera "ola", pues en ninguno de los dos tipos de ataque restantes hubo respuestas; más bien, la cantidad de correos enviados podría influir con la detección del correo de *phishing*. Lo anterior se deduce porque en cada "ola" alguna persona detectó el ataque. Por otro lado, se detectó más el caso del correo de ataque con diversidad que el correo sin diversidad, lo cual resulta un dato interesante.

Del experimento pude concluir que el ataque sin diversificación fue más efectivo; además, el resultado refleja un alto desconocimiento de medidas de ciberseguridad para detectar *phishing* por parte de los funcionarios. Esto último preocupa pues los funcionarios, a pesar de ser todos profesionales, presentaron un nivel de respuesta muy alto (el 50% respondió). A raíz de esta situación, se buscó generar conciencia del tema, brindando información al respecto a cada empleado para que tomara las precauciones del caso y evitar futuros hechos de este tipo cuando realmente un cibercriminal actúe.

Conclusiones

De acuerdo con lo investigado, se concluye que el factor humano sigue siendo el eslabón más débil, ¿de qué sirven todas las medidas técnicas de protección si al final el usuario brinda la

información sensible o privada? lo cual hace necesario que las empresa e instituciones trabajen el tema de cultura digital, pues se evidenció que el personal no está preparado para acciones de ciberdelincuencia, y es muy probable que muchas instituciones del estado se encuentren bajo la misma situación o estén vulneradas sin haberse percatado.

Es necesario desarrollar una cultura de seguridad de la información, tener un plan de recuperación de desastres y un plan de respuestas a incidentes; el pensar que nunca les va a pasar algo no es una buena idea, por lo que deben buscar protegerse. La ingeniería social, y en específico el phishing, en muchos de sus variantes, pueden evitarse creando una cultura personal de concienciación, pero es necesario que la seguridad de la información y la ciberseguridad sean considerados un tema medular.

Referencias bibliográficas

Hadnagy, C. (2011). Ingeniería Social el arte del hacking personal. Madrid, España. Ediciones Anaya Multimedia

Instituto Nacional de Ciberseguridad de España (INCIBE). Kit de concienciación, https://www.incibe.es/empresas/Kit_de_concienciacion/

Gutierrez, H.; De la Vara, R. (2008). Análisis y Diseño de Experimentos. México. Mcgraw-Hill Interamericana

De Luz. S. (mayo 2016). Aumenta el spam malicioso en el primer trimestre del 2016 según el informe de Kaspersky. Redes Zone http://www.redeszone.net/2016/05/29/aumenta-spam-malicioso-primer-trimestre-del-2016-segun-informe-kaspersky/

Sandoval, E. Ingeniería Social: Corrompiendo la mente humana. Revista Seguridad UNAM 10 http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

Padilla, Miriam. Pescando Información Phishing. Revista de Seguridad UNAM 02 http://revista.seguridad.unam.mx/numero-02/pescando-informaci%C3%B3n-phishing

Lozano, A. (2009). Análisis teórico-experimental de técnicas y herramientas de phishing y delitos electrónicos http://e-archivo.uc3m.es/bitstream/handle/10016/5819/PFC_Abel_Lozano_Prieto.pdf?sequence=1&isAllowed=y

Jiménez,M. Introducción a Social-Engineering Toolkit (SET). Hack Players http://www.hackplayers.com/2012/10/social-engineering-toolkit-set.html

Sobre el autor:

Roberto Lemaître Picado es Máster de la Maestría Profesional en Computación e Informática de la Universidad de Costa Rica, Licenciado en Derecho por la Universidad de Costa Rica, Ingeniero Informático por la Universidad Estatal a Distancia y Técnico en Computación por el Colegio Vocacional Monseñor Sanabria. Es consultor en temas de derecho informático, protección de datos y seguridad de la información, brindando distintos talleres, foros, capacitaciones y asesorías en la materia. Ha participado en diversas actividades y talleres relacionados con el derecho y las tecnologías, tanto a nivel nacional como internacional, además, tiene diversas publicaciones referentes a ciberseguridad y derecho informático. Ha sido entrevistado en muchas ocasiones por medios periodísticos nacionales e internacionales sobre temas relacionados con la materia de ciberseguridad, protección de datos, derecho informático, entre otros. Miembro de Internet Society. Representante para Costa Rica en la Red Iberoamericana de Derecho Informático. Representante para

Costa Rica en el Observatorio Iberoamericano de Legislación y Políticas TIC. Colaborador de la iniciativa del Observatorio Iberoamericano de Protección de Datos. Miembro del Consejo Consultivo Internacional de la Academia Mexicana de Derecho Informático, A.C. Ha sido Profesor en la Universidad de Costa Rica y de la Universidad Técnica Nacional en las Escuelas de Computación e Informática. Conferencista invitado en distintas universidades del país. Fue seleccionado por el periódico El Financiero entre las 40 personas valiosas menores de 40 años que ha realizado valiosos aportes en su área en el país. Reconocimiento Abogado Destacado 2017 de la Red Iberoamericana de Derecho Informático. Premio al Mérito Informático 2017 en la categoría Pionero, del Colegio de Profesionales en Computación e Informática, CPIC. Fundador y director del programa por internet Noches de Ciberseguridad. Actualmente funge como Coordinador Centro de Respuestas de Incidentes Informáticos de Costa Rica CSIRT-CR, Ministerio de Ciencia, Tecnología y Telecomunicaciones

CC BY SA

CyberSecurity
Información & Privacidad

Manejo De Malware Destructivo

Destructive Malware Management

Mauricio Pérez
email: manngt@gmail.com
Recibido:15/enero/2020. Revisado: 22/febrero/2020. Aprobado: 1/Junio/2020.
Disponible en internet el 1 de abril de 2020

Resumen: Un sistema de gestión de la seguridad de la información tendrá como objetivo implementar metodologías, procedimientos, protocolos, auditorías entre otras actividades para poder disminuir los riesgos a los que se enfrentan las empresas, riesgos que podrían representar una gran amenaza interna, para ello se determina la probabilidad haciendo un análisis de los incidentes y su ocurrencia, siendo un factor importante darle prioridad a aquellos riesgos que son muy probables que se materialicen, además del nivel de impacto al analizar las consecuencias que podrían volverse realidad al no controlar los riesgos. Las consecuencias dependen de los recursos que sean de gran valor para una empresa. Entonces la seguridad de la información tendrá como objetivo primordial la prevención y disminución de los riesgos.

Palabras Claves: programa malicioso, nivel de impacto, ciberseguridad, incidentes, prevención.

Abstract: An information security management system will aim to implement methodologies, procedures, protocols, audits, among other activities, in order to reduce the risks that companies face, risks that could represent a major internal threat, for which it is determined the probability making an analysis of the incidents and their occurrence, being an important factor to give priority to those risks that are very likely to materialize, in addition to the level of impact when analyzing the consequences that could become reality by not controlling the risks. The consequences depend on the resources that are of great value to a company. Then information security will have as its primary objective the prevention and reduction of risks.

Desarrollo:

Independiente de nivel de sofisticación que tenga el malware al final importará el impacto que ocasione en el ecosistema que llego a vulnerar en la organización, al integrar la seguridad de la información a la estrategia corporativa se incrementan los niveles de prevención y protección entonces el resultado será una minimización del riesgo, sin embargo, no se debe subestimar el residuo del riesgo, porque por mínima que sea su probabilidad el impacto podría ser alto y si existe ocurrencia será suficiente para poner en situaciones catastróficas a las empresas. Aunque se reduzcan los riesgos al mínimo se deben de considerar las situaciones que tienen baja probabilidad de ocurrir.

Entonces también será una actividad de la seguridad de la información crear la gestión de respuesta ante cualquier riesgo de carácter destructivo. Dando origen a varios aspectos que definirán la mejor respuesta a situaciones que pongan en peligro la integridad, disponibilidad y privacidad de la información. Como parte de la preparación de una gestión de respuesta hay aspectos que deben existir y así tener un mínimo de control ante estas situaciones:

Definición de la prioridad de la seguridad de la información: Basado en la estrategia y objetivos de la empresa al estar operando con normalidad existirá una prioridad jerárquica de la integridad, confidencialidad o disponibilidad. Por ejemplo, un banco donde ocurren muchas transacciones desde diferentes orígenes podría definir como prioridad la alta disponibilidad, seguido estará su integridad y por último su confidencialidad, sin discriminar la importancia de cada una. Al ocurrir una infección que busque extraer información se puede establecer que al estar identificada y certificada la ocurrencia la prioridad sería la confidencialidad y disponer que no exista la disponibilidad por un tiempo estipulado hasta que se logre certificar que la información estará protegida al máximo.

Identificación de recursos y dispositivos: La seguridad de la información contempla este aspecto, para esta planeación, adicional contemplar aquellos recursos de información y dispositivos que serán un pilar para una respuesta efectiva ante cualquier incidente.

Recurso Humano: Dentro de la planeación serán de alta importancia los especialistas de cada sistema, dispositivo y principalmente aquellos expertos en situaciones donde han ocurrido infecciones y que el nivel de propagación e impacto han sido elevados. Cada especialista aportará elementos a considerar que son vitales ante situaciones de este tipo. También podrán indicar qué actividades deben realizarse con el objetivo de detener la propagación e impacto. Tanto lo que puede, debe hacerse o lo que no debe hacerse. Deben contemplarse aquellos asesores que pueden involucrarse y definir un contrato para que asistan al ocurrir un incidente.

Definición de síntomas: Indicadores para incidentes de infección para casos conocidos, además de establecer mecanismos que puedan identificar comportamiento de actividades de software destructivo.

Elementos de monitoreo: Tendrán como principal objetivo informar de comportamiento atípico dentro de la red y los sistemas. También de ir registrando la disponibilidad de los recursos y así tener una métrica del avance del impacto. Las bitácoras de los sistemas deberán centralizarse y protegerse para determinar qué está ocurriendo y como está sucediendo.

Protección de recursos de respuesta: Definir cómo proteger aquellos recursos de información y dispositivos para que estén disponibles en el momento de ocurrencia del evento. Es vital porque de ello depende de las decisiones que se tomen el momento del incidente.

Normas: Definir las reglas, autoridad y autorización en escenarios donde ha sobrepasado los controles de seguridad y se está esparciendo.

En situaciones caóticas es importante mantener el orden y la organización en los planes que se están aplicando, principalmente con escenarios donde se están tratando con programas malignos destructivos y que el impacto podría ser alto y que sus consecuencias devastadoras.

La estrategia permitirá tener un control global de lo que se está realizando y así poder determinar el avance de respuesta al incidente. La táctica permitirá definir la mejor forma de realizar las actividades y procedimientos, por ello la importancia de incluir a diferentes actores con la experiencia suficiente para determinar una ejecución eficiente de las actividades y tareas.

Al ocurrir un incidente de infección el plan de respuesta deberá considerar como prioridad la prevención de infección total de los sistemas, seguido de esto contener y aislar los sistemas

infectados. Paralelo a las acciones de prevención y contención deberán realizarse aquellas actividades para eliminar la amenaza y recuperar la operación con mínima pérdida de información.

Es de gran importancia la preparación ante situaciones no importando su probabilidad de ocurrencia. En la mayoría de los casos se desconoce cuándo ocurrirá por primera vez y por eso no basta con hacer un análisis de probabilidad. Se deben incluir análisis que permitan identificar las amenazas a los que se está expuesto, aunque no exista la probabilidad de ocurrir. El análisis permitirá la creación de planes de respuesta que podrán variar según las amenazas identificadas.

Los planes de respuesta tendrán un orden de prioridad, iniciando con prevención de infección en los recursos no afectados, después se pondrán en cuarentena aquellos que están sufriendo de infección y para finalizar será la desinfección. El objetivo primordial será el recuperar la funcionalidad con la mínima pérdida de datos.

Referencias bibliográficas

Stewart, J. M., Chapple, M., & Gibson, D. (2015). Certified Information Systems Security Professional Study Guide (7ª ed.). Indianapolis, Indiana, US: SYBEX.

Mathew, M. (2014). Introducción a la programación (2ª ed.). México: Grupo Editorial Patria.

Baum, J. (1986). The Calculating Passion of Ada Byron. London:Archon Books

Aycock, J. (2006). Computer Viruses and Malware. Canada: Springer

Sobre el autor:

Administrador de sistemas con 20 años de experiencia en proyectos de Infraestructura Tecnológica, participación en proyectos de comunicaciones unificadas, planes de recuperaciones de desastres, plataformas de gestión de contenido, automatización de sistemas entre otros. Programador independiente en plataformas web y móviles.

CyberSecurity
Información & Privacidad

DMARC - un paso adelante para proteger la reputación de la empresa

DMARC - a step forward to protect the company's reputation

Rodrigo Calvo
email: orionx.rc@gmail.com
Recibido: 14/mayo/2020. Revisado: 29/junio 2020. Aprobado: 18/julio/2020.
Disponible en internet el 1 de septiembre de 2020

Resumen: DMARC es un protocolo de autenticación de correo cuya aplicación ha aumentado en los últimos cinco años dado sus beneficios para mitigar ataques que suplantan la identificación del remitente. Los Servidores de Nombres de Dominio (DNS) y los servidores de correo que inician el mensaje así como los que reciben son la cadena que sostiene al protocolo. Se presentará en el artículo un resumen de ciertas características de la autenticación y así como un pequeño análisis de su uso. Con fines de identificar la situación actual se seleccionaron 78 dominios de correo pertenecientes a empresas e instituciones en cuatro países de Centroamérica. Se compararon en esos dominios el uso o no de DMARC en distintas áreas. El uso de DMARC debe encontrarse dentro de los procesos operativos de las empresas hasta culminar con la política de rechazo, esto ayudará a bajar una gran incidencia uso no autorizado de los dominios de correo.

Palabras Claves: BEC, Email Spoofing, DMARC,DKIM,SPF.

Abstract: DMARC is an email authentication protocol whose application has improved over the past five years given its benefits in mitigating attacks that impersonate sender identification. The Domain Name Servers (DNS) and the mail servers that initiate the message as well as those that they receive are the chain that maintains the protocol. A summary of specific characteristics of authentication and a brief analysis of its use will be presented in the article. With fines to identify the current situation, 78 email domains belonging to companies and institutions in four Central American countries can be selected. The use or not of DMARC in different areas were compared in these domains. The use of DMARC must be within the operating processes of companies until culminating in the rejection policy, this is what requires a low incidence of unauthorized use of email domains.

Desarrollo:

La comunicación mediante correo electrónico se ha mantenido en aumento constante desde su origen en los años setenta, no obstante, esto ha traído inherentes usos maliciosos con el pasar del tiempo. De forma casi natural surgió el correo no deseado (SPAM), el cual, satisfacía objetivos comerciales de los más variados gustos sin respetar la decisión del receptor de aceptar los correos o no. Surgen entonces propuestas de defensa llamadas Gateways de SMTP con capacidades ANTI-SPAM y como bola de nieve se desarrollan estrategias organizadas para atacar las plataformas de mensajería de formas diferentes.

Los dominios de correo no sólo se volvieron puntos de identificación sino también de reputación en el mercado para clientes, instituciones y empresas. Conociendo lo anterior, y bajo psicología de ingeniería social encontramos mecanismos de falsificación del origen de

correo para realizar solicitudes a nombre de alguien más y de ahí obtener una ganancia. Un ejemplo claro, es que al conocer la transaccionalidad de pagos de una empresa hacia uno o más proveedores, un cibercriminal puede influir en la ejecución del pago a través de un simple correo electrónico si este se visualiza que fue enviado por el proveedor, a esto se le llama en inglés Business Email Compromise.

La falsificación de correo requiere conocer la estructura técnica del mensaje, la parte técnica y no visible a través del cliente de correo se le llama "Sobre" (Envelope), el siguiente componente es el Encabezado (Header) el cual lo encontramos visible en las aplicaciones de correo (Web o tipo Outlook).

Los protocolos de autenticación vigentes en el 2020 basan su efectividad en los siguientes parámetros: Envelope (RFC5321): Envelope-Sender , también llamado Return-Path o bien MFROM y Header (RFC5322): Header From

En 2019, en el reporte de Crimen en Internet publicado por el Internet Crime Complaint Center (IC3) se consignó la alarmante cantidad de $1.7 mil millones en pérdidas por concepto de estafas a través de correo electrónico. A Centroamérica no le ha sido distinto el panorama. Entre el 1º de abril 2019 al mismo mes en 2020 el Organismo de Investigación Judicial de Costa Rica registró 588 casos relacionados con estafa informática y suplantación de identidad, que si bien la estadística no es directa sobre el uso de correo si deja a entrever el mecanismo criminal en aumento. A la par del registro de delitos informáticos también crece una sombra de lo no declarado, dado que muchas empresas se reservan su derecho para denunciar el ilícito. La reputación de la empresa usualmente es la barrera que la aleja de estas instancias judiciales.

Ante un aumento de suplantación de identidad en plataformas de correo electrónico el reto para las empresas consiste en proteger su marca y su reputación. DMARC es el punto de partida. La estandarización de procesos de autenticación a través del protocolo DMARC se mantiene evolucionando y el objetivo a alcanzar es proveer de suficiente criterio a ISPs y plataformas de correo para identificar la autenticidad de la fuente del correo electrónico. La administración de la seguridad de la información es uno de los grandes problemas de las organizaciones. Se depende de administradores y analistas de seguridad para mantener las distintas capas de información aseguradas. Los especialistas de Seguridad Informática deben administrar los valores de las empresas manteniendo la confidencialidad, integridad y disponibilidad de la información.

¿Qué es DMARC?

Es una técnica de autenticación de correos electrónicos apoyada sobre la base de dos protocolos maduros conocidos como SPF y DKIM. Publicado en 2012, su aceptación de forma masiva ha aumentado en los últimos cinco años.

Los servicios de recepción de correo evalúan la política que el remitente ha establecido para su DMARC y de forma eficiente pueden clasificar el correo para ser enviado a un folder de cuarentena o bien rechazar de plano el correo.

Entre los beneficios de una implementación correcta están: **Reducción de Falsos Positivos**: la cuarentena es dirigida por la falta de alineamiento con la política. **Reportes de Autenticación**: el diseño prevé el envío de reportes que enumeran errores de autenticación y las direcciones IP desde donde se originó el correo. **Protección bidireccional**: la política beneficia la reputación del remitente, así como brinda confianza del correo recibido en el receptor. **Mitigación de Spoofing y Business Email Compromise**: al incrementarse las opciones para verificar la legitimidad del remitente. **Escalable**: Servidores de Correo, Gateways de SMTP y DNS permiten la combinación de factores para la eficiencia del proceso de autenticación.

Sender Policy Framework (SPF) Define cuales servidores de correo están autorizados para enviar correo a nombre del dominio origen.

DomainKeys Identified Mail (DKIM) Permite mediante el uso de criptografía asimétrica autenticar el origen del correo.

La unión hace la fuerza SPF+DKIM = DMARC

DMARC brinda las indicaciones para los servidores que reciben correo para que determinen si el mensaje se puede aceptar, enviar a cuarentena o incluso rechazar de plano, a través del uso de SPF y DKIM. Ver figura 1.

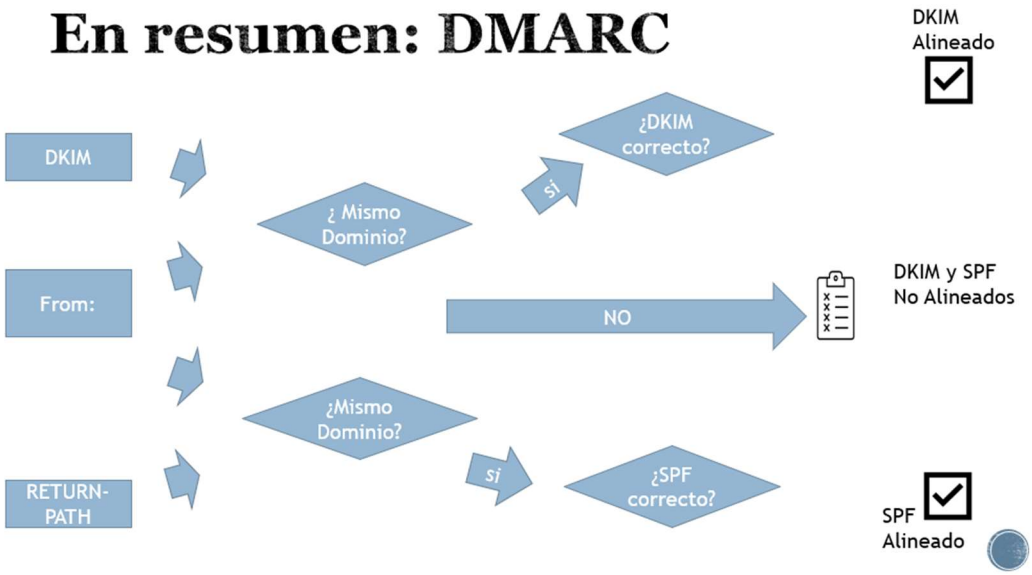


Figura 1. Flujo de análisis DMARC

Uso de DMARC en Centroamérica

Se analizó una lista de 78 dominios de correo de empresas localizadas en Guatemala, Honduras, Costa Rica y Panamá con el fin de verificar si el uso de DMARC se ha extendido en la región. Los resultados pueden no sorprender en muchos casos y en otros llamó la atención los errores comunes en el registro publicado.

El 60% de los dominios evaluados no contaban con política DMARC definida lo cual puede indicar desconocimiento de las facilidades que se alcanzan. Ver figura 2.

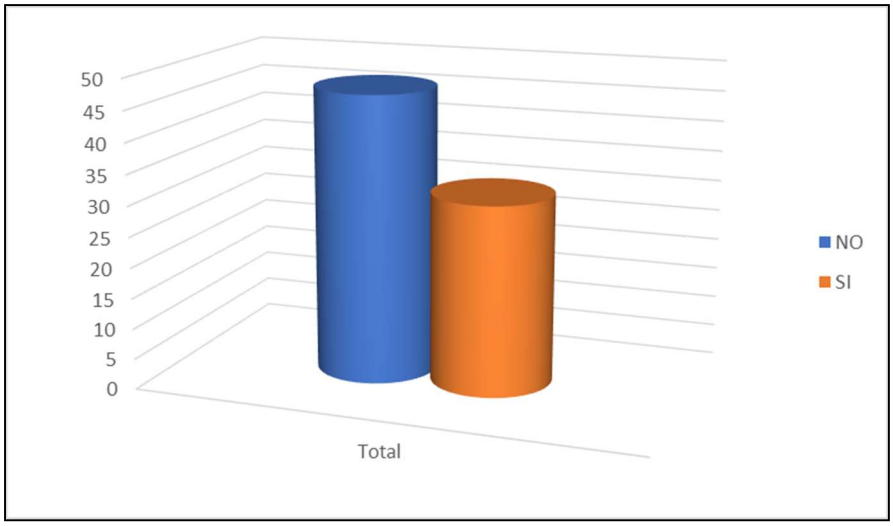


Figura 2. Brecha de uso de DMARC

De 31 dominios que están usando la política el 10% usa una dirección asociada a una persona para recibir los reportes de los ISP, sin embargo, no es una práctica recomendada, lo ideal sería el uso de un alias tal como rua@sudominio.com. Un 12% muestran errores de sintaxis o no usan casillero para RUA del todo. Ver figura 3

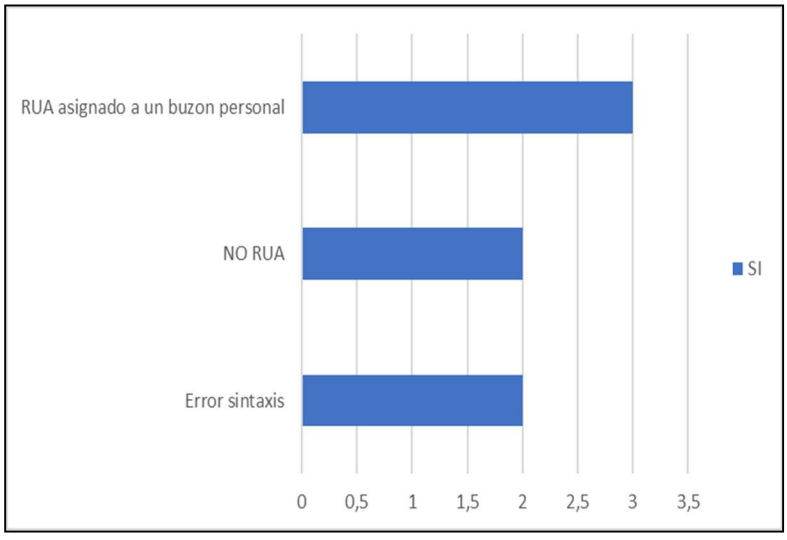


Figura 3. Errores comunes en implementación

De la figura siguiente se infiere que el uso de DMARC en instituciones Públicas es más frecuente que en el área privada.

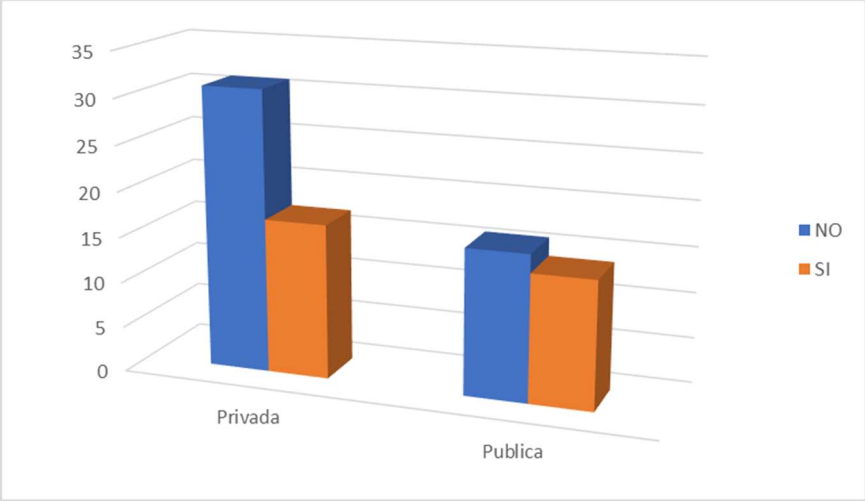


Figura 4. Uso de DMARC por Área

El sector financiero presentó evidencia sólida de al menos una política de monitoreo establecida respecto a otros sectores.

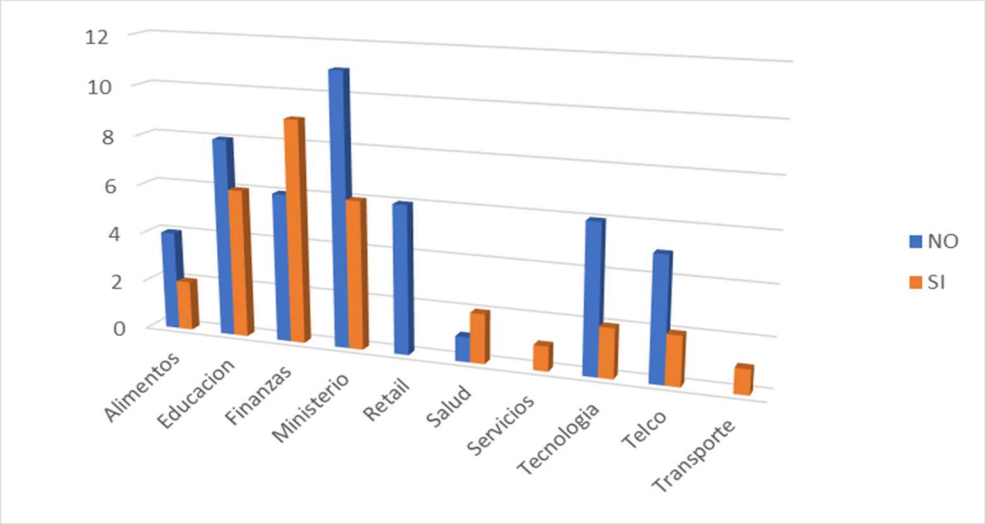


Figura 5. Uso de DMARC por Sector Productivo

Del conjunto de empresas o instituciones que están usando DMARC el 50% se encuentra aplicando la política de cuarentena, 47% aplica Monitoreo y un 3% usa “reject”.

Del grupo de Monitoreo se puede inferir que en el mejor de los casos podría estar iniciando en el proceso de DMARC y en el peor escenario dejó monitoreo por defecto sin revisarlo periódicamente.

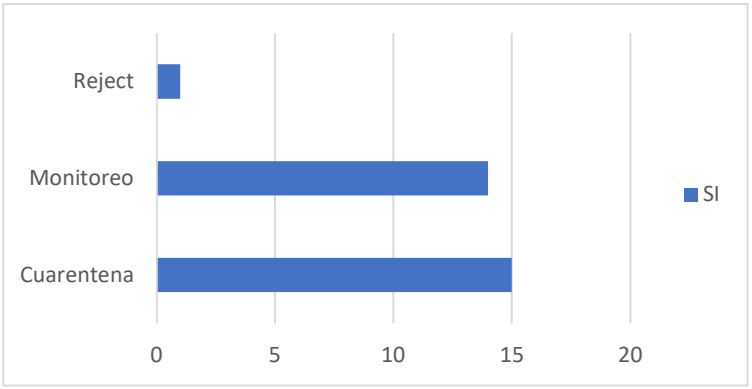


Figura 6. Uso de Política DMARC

PASOS PARA IMPLEMENTAR DMARC

En el nivel de Empresa: Investigar con las áreas de Mercadeo, Investigación y Relaciones Públicas si hacen uso de algún recurso de envío masivo de correo electrónico no corporativo en el cual el MailFrom use el dominio de la empresa. Si fuera así la política por defecto debería ser NONE, dado que les dará tiempo a los encargados de implementar DMARC para entender restricciones de subir la política al nivel de Cuarentena. Identificar si existen dominios adquiridos por departamentos diferentes a Tecnologías de la información que no sean usados para envío de correo.

A nivel de Departamentos de Tecnología y Seguridad: Definir un encargado de cumplimiento de DMARC que revise las herramientas y reportes de RUA, generados diariamente. Establecer como política por defecto “Reject” a todos aquellos dominios adquiridos en la empresa que NO sean usados directamente para envío de correo. La razón es que estos dominios cuando son identificados por terceros son usados para ataques tipo BEC. Presupuestar la adquisición de servicios de análisis de reportes RUA o bien asignar la labor de revisión de los archivos xml de forma periódica (la cantidad de reportes es muy alta por lo cual no se sugiere esto último). Usar por defecto la política “none” para aquellos dominios que sean usados para envío de correo. El objetivo es generar reportes que permitan identificar errores que deben ser arreglados en no menos de tres meses. Asignar la política “Quarantine” (cuarentena) o “Reject” cuando haya certeza de menos de un 1% de errores DMARC. Definir un control de cambio con los encargados de administrar el DNS de la empresa para incluir registros SPF,DKIM y DMARC. Usar herramientas gratuitas para verificar de encabezados de correo y de registros SPF,DKIM,DMARC o bien las que facilite el proveedor de análisis de reportes RUA. Entre las herramientas gratuitas ampliamente usadas están:

https://mxtoolbox.com/dmarc.aspx , https://mxtoolbox.com/EmailHeaders.aspx , https://dmarcguide.globalcyberalliance.org/ , https://stopemailfraud.proofpoint.com/dmarc/ https://dmarcian.com/dmarc-inspector/

CONCLUSIONES

DMARC es un beneficio para las instituciones públicas o privadas, en términos de reputación y de mitigación de riesgos de falsificación de correos, sin embargo, requiere trabajo operativo y de análisis de reportes.

Seguir el protocolo no sólo implica ajustar los parámetros para un "monitoreo permanente" sino también determinar el momento oportuno para asignar la acción de "rechazo" (reject) y así minimizar los ataques tipo BEC.

De acuerdo con el estudio realizado se determinó que hay una excelente oportunidad de mejora en Centroamérica para ampliar el uso de DMARC y llevarlo a un nivel de seguridad de integridad más completo que el existente.

Si bien la implementación podría verse como gratuita, el análisis de reportes requiere invertir para poder sacar provecho de la asignación de políticas a corto y mediano plazo.

Referencias bibliográficas

Internet Crime Complaint Center. (2020, 4 de Septiembre). 2019 Internet Crime. Disponible en https://pdf.ic3.gov/2019_IC3Report.pdf

Internet Engineering Task Force ,IETF .(2008, Octubre). Simple Mail Transfer Protocol. Disponible en: https://tools.ietf.org/html/rfc5321

Internet Engineering Task Force ,IETF. (2008, Octubre). Internet Message Format. Disponible en: https://tools.ietf.org/html/rfc5322

DMARC.org. DMARC Overview. Disponible en: https://dmarc.org/overview/

Global CyberAlliance.org. Enter your domain to start the DMARC Setup. Disponible en: https://dmarcguide.globalcyberalliance.org/#/

Sobre el autor:

Consultor Internacional de Ciberseguridad con más de 15 años de experiencia, Certificado e Instructor Autorizado en Information Systems Security Professional (CISSP) así como de Ethical Hacker (CEH) , profesor en la Maestría de Ciberseguridad de la Universidad Cenfotec en Costa Rica, Miembro de la Junta Directiva del Capítulo (ISC)2 Costa Rica, Speaker en Congresos de Protección de Datos y Ciberseguridad, actualmente labora como Arquitecto Senior de Seguridad de la Información en la compañía Infolock, Virginia , Estados Unidos , anteriormente fue Sr. Security Engineer en Symantec Corp Latinoamérica.

CyberSecurity
Información & Privacidad

Guía de negocios básicos - Prevención de fraudes en línea

Basics Business Guide - Online Fraud Prevention

Fraudwatch International - Trent Youl
email: trenty@fraudwatchinternational.com
Recibido: 1/abril/2020. Revisado: 20/junio 2020. Aprobado: 01/julio/2020.
Disponible en internet el 1 de septiembre de 2020

Resumen: El fraude en línea es una de las amenazas crecientes para las empresas con presencia digital. Con un costo de millones de dólares cada año, este tipo de ataque es definitivamente algo para tener en cuenta, por lo que la prevención del fraude en línea es una necesidad. Aprenda lo que puede hacer para prevenir el fraude en línea y cómo recuperarse si se convierte en una víctima de él. El fraude en línea es un tipo de delito cibernético, en el que los delincuentes engañan a las víctimas para que proporcionen sus datos personales, que luego utilizan para robar dinero o llevar a cabo actividades fraudulentas. Hay diferentes maneras en las cuales se realiza el fraude en línea, como la venta de tarjetas digitales de regalo falsas, ofreciendo entradas falsas para conciertos y eventos deportivos, y por supuesto, la ejecución de estafas en las plataformas de medios sociales. Según una investigación, solo en 2017, las víctimas perdieron más de $ 1.4 mil millones por fraude en línea. Esta cifra está creciendo constantemente, dejando a los propietarios de negocios sin más remedio que implementar un plan de prevención del fraude en línea dentro de su organización.

Palabras Claves: Fraude, victimas, prevención, ataques.

Abstract: Online fraud is one of the growing threats for businesses with a digital presence. Costing millions of dollars every year, this attack type is definitely something to watch out for, so online fraud prevention is a must. Learn what you can do to prevent online fraud, and how to recover if you become a victim of it. Online fraud is a type of cybercrime, in which criminals mislead or deceive victims into providing their personal details, which they then use to steal money or carry out fraudulent activity. There are different ways to perform online fraud, such as selling fake digital gift cards, offering fake tickets to concerts and sport events, and of course, running scams on social media platforms. According to research, in 2017 alone, victims lost over $1.4 billion to online fraud. This figure is steadily growing, leaving business owners with little choice but to implement an online fraud prevention plan within their organisation.

Desarrollo:

La mayoría del fraude en línea se puede dividir en dos escenarios principales: **Enfocado al cliente**: este escenario generalmente se realiza a través de ataques de phishing contra clientes, robando su información y usándola para hacerse cargo de sus cuentas para realizar compras fraudulentas u obtener sus datos financieros. **Enfocado al negocio**: este escenario requiere cambiar algo administrado por el negocio, como el sitio web. Un ejemplo notable de esto es 'Magecart', un grupo de delitos cibernéticos dirigido a sitios web minoristas con un script de ladrón de tarjetas de crédito insertado en el código fuente del sitio web.

Pero ¿cómo pueden las empresas abordar con éxito el fraude en línea? ¿Y puede prevenirse por completo? Bueno, en ciberseguridad no existe una protección 100% infalible, pero algo de protección es mejor que nada.

Hay varias medidas que las empresas pueden implementar en sus sitios web para minimizar el riesgo, monitorear los intentos de fraude y mejorar en gran medida su protección contra el fraude en línea:

- El número de intentos de entrada de la tarjeta de crédito. Si un cliente intenta insertar diferentes números de tarjetas de crédito más de un par de veces es sospechoso, e implica un estafador está detrás de la compra.

- Comprobaciones adicionales. Ejecute comprobaciones adicionales en las compras en las que la dirección de facturación difiera de la dirección de envío, especialmente si el cliente eligió el envío rápido. Esto no es un signo definitivo de un fraude, pero vale la pena contactar al cliente con los detalles que tiene (número de teléfono, correo electrónico, etc.) verificar.

Esto también se aplica a otras transacciones sospechosas:

- Actualizar el software que está utilizando para la última versión. Se descubren errores y agujeros de seguridad en todo el software, por lo que la actualización minimiza. regularmente las posibilidades de que los hackers puedan explotar vulnerabilidades en su sitio web.

- Compruebe regularmente el código fuente de su sitio. Se debe realizar un análisis cuidadoso del código fuente de su sitio web a intervalos regulares para ver si se ha insertado algo nuevo en él. Como se explicó anteriormente, este es el método preferido del famoso grupo de delitos cibernéticos Magecart y es utilizado por otros delincuentes cibernéticos también.

¿Cuánto vale el negocio de fraude en línea para los ciberdelincuentes? Las estadísticas muestran que su valor es bastante alto. En Australia, por ejemplo, casi AUD $ 5 millones fueron robados en 2019 como resultado de 10.000 diferentes incidentes de estafas de compras en línea.

En los Estados Unidos, el 77% de los comerciantes dice haber sido víctima de algún tipo de fraude en línea y que las transacciones fraudulentas representan un promedio del 27% de sus ventas anuales en línea. A nivel mundial, la estimación es que la ciberdelincuencia costará alrededor de US $ 6 Billones el año 2021, y el fraude en línea tomará una gran parte del pastel. Por lo tanto, vamos a recapitular lo que las empresas pueden hacer para mejorar su prevención del fraude en línea:

- El número de intentos de entrada de la tarjeta de crédito.

- Verificación de las transacciones.

- Software regularmente actualizado.

- Código fuente de su sitio modificado por partes no autorizadas.

Para proteger a su marca y clientes del fraude en línea, FraudWatch International ofrece un servicio de monitoreo utilizando software propietario. Nuestras herramientas buscan incidentes fraudulentos en Internet y realizamos derribos, cuando corresponda. De hecho, tenemos algunos de los tiempos de derribo más rápidos a nivel mundial con una tasa de éxito del 100%.

Referencias bibliográficas

Cyber Security Hub (2016, November) https://www.cshub.com/events-cybersecurity-exchange/sponsors/fraud-watch-online-1

FBI USA (2015, June) https://www.fbi.gov/investigate/cyber

FraudWatch International: Cyber Security Services & Solutions (2018, March) fraudwatchinternational.com

Oficina de Seguridad del Internauta (2020, March) https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen

Statista (2019 August) https://www.statista.com/topics/2588/us-consumers-and-cyber-crime/

Sobre el autor:

Trent Youl es el fundador y director ejecutivo de FraudWatch International, una compañía de seguridad global de Internet de propiedad privada que se centra en la protección contra la suplantación de identidad y la marca en línea desde 2003. Trent ha desarrollado la compañía y sus servicios proactivos, desde un pequeño negocio doméstico hasta un negocio global con oficinas en Melbourne, Londres, Dubai y San Francisco, atendiendo a clientes en más de 35 países de todo el mundo.

Trent controla todas las áreas del negocio y tiene un enfoque práctico en el desarrollo continuo de los servicios para proteger mejor a los clientes del abuso de marca en línea. Trent tiene un enfoque en el análisis de phishing y abuso en línea, asociaciones estratégicas de negocios y desarrollo de negocios globales.

CC BY SA

INSTITUTO NACIONAL DE CIBERSEGURIDAD DE GUATEMALA

INCIBE GT

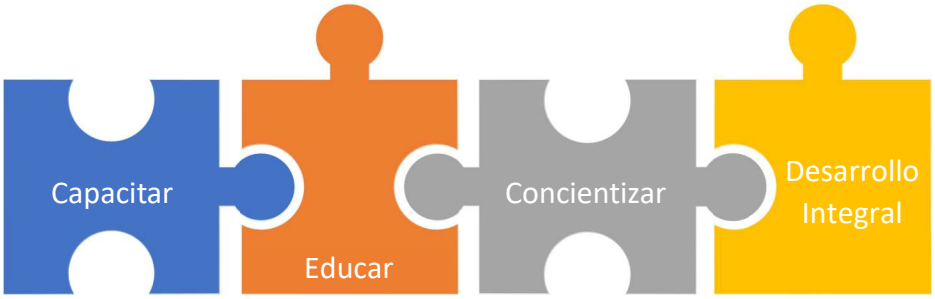
Somos una organización sin fines de lucro, creada con la misión de incentivar la educación, capacitación, concientización, mejores prácticas en temas de tecnología y ciberseguridad en Guatemala. Nuestros proyectos están orientados a apoyar y dar seguimiento a toda la ciudadanía, organizaciones e instituciones que lo requieran a través del uso innovador de las tecnologías.

INCIBE GT nace de lo indicado por la Estrategia Nacional de Seguridad Cibernética en el Eje de Educación para ofrecer ofertas educativas y formativas sobre seguridad y desarrollar e implementar programas de investigación y desarrollo. Al ser una Organización sin Fines de lucro, nos debemos a Financiamiento local o internacional de entidades del gobierno, ONGs, empresas privadas para llegar a cabo nuestros proyectos.

NUESTROS PROYECTOS

En INCIBE GT buscamos apoyar por medio de la tecnología a los ciudadanos, organizaciones de gobierno e instituciones a crear soluciones y proyectos que los ayuden a mejorar la privacidad de la información, además conectar y unir los esfuerzos del país en búsqueda de una seguridad de datos que aporten bases sólidas para todos los ciudadanos del país, dentro de estos CiberSecGT, proyecto creado como un apoyo a Universidades en Guatemala para realizar capacitaciones y eventos que impulsen la seguridad de la información, además la primera revista digital orientada a ciberseguridad denominada “Cybersecurity – Información y Privacidad”, la cual cuenta con ISBN e ISSN y en proceso de indexación con la Universidad de San Carlos de Guatemala, apoyando con artículos científicos de autores guatemaltecos que promuevan una concientización en el uso de tecnologías y minimizar ataques tecnológicos a la integridad de ciudadanos, organizaciones y empresas. RoboKids Guatemala, emprendimiento que apoya a niñas, niños y adolescentes con metodologías STEAM para talleres sobre robótica y seguridad en el internet.

NUESTROS EJES



NUESTROS AMIGOS

INCIBE Guatemala cuenta con lectores, autores, comunidades y fundaciones sin ánimo de lucro que nos apoyan a impulsar y mejorar la calidad de la sociedad de la información en Guatemala.

NUESTRAS ALIANZAS

INCIBE Guatemala realiza esfuerzos para crear alianzas con entidades del Gobierno, No Gubernamentales y Privadas para apoyar la concientización, privacidad y aseguramiento de los datos en los ciudadanos del país.

FINANCIAMIENTO

Al ser una Organización sin Fines de lucro, nos debemos a Financiamiento local o internacional de entidades del gobierno, ONGs, empresas privadas para llegar a cabo nuestros proyectos.

LATAM Women in Cybersecurity

WOMCY

En las escuelas de Ingeniería de Sistemas e Informática, en las grandes universidades del mundo, podemos observar, de acuerdo con las estadísticas, el alto índice de participación de alumnos de género masculino (68,24%)* contra la poca participación de alumnos de género femenino (31,75%)*, lo que ha sido una variable fija, durante muchos años.

Las carreras STEAM, consideradas por muchos 'las carreras del futuro', son una opción minoritaria entre los programas con mayor cantidad de egresados en muchas universidades. Aunque las mujeres estudian programas técnicos, tecnológicos universitarios y postgrados, relacionados con las áreas STEAM, la participación femenina porcentual frente a los hombres se mantiene en una proporción de 3 mujeres por cada 10 egresados en los últimos 17 años*.

En las últimas décadas, la mujer, ha ido incursionando en varios campos de la vida profesional, destacándose en el área de las ciencias y las matemáticas. El área de la tecnología no se ha quedado atrás, por ello y por la necesidad de conseguir mayor participación en este campo, en sus diferentes ramas, legal, ciberseguridad, apoyo educativo, asesoría laboral entre otros, es por lo que un grupo de mujeres con amplia experiencia en el campo de la CIBERSEGURIDAD, decidieron crear una organización sin fines de lucro, que uniera mujeres con intereses comunes. Es así como nace WOMCY.

WOMCY, es una organización sin fines de lucro, conformada por mujeres, con foco en el desarrollo de la Ciberseguridad en Latinoamérica, teniendo su base legal y administrativa en Estados Unidos. Recientemente, hemos abierto las puertas de la organización a hombres, quienes en la búsqueda de aportar experiencia, conocimiento y diversidad, ingresaron, creándose así el equipo 'WOMCY He for She'. Así mismo, tenemos los equipos de WOMCY Marketing, WOMCY Legal, WOMCY Alliance, WOMCY Membership y el de WOMCY Volunteering, los cuales sirven como apoyo a la ejecución de nuestros programas.

Su objetivo es "Minimizar la brecha de conocimiento y la carencia de talentos en Ciberseguridad, a nivel de Latinoamérica". Tenemos Programas, que fortalecen la presencia de WOMCY, dentro de las comunidades, como por ejemplo para el sector Educativo para los cuales tenemos WOMCY Girls y WOMCY Geek; para Universidades, WOMCY Jobs y WOMCY Tech. En el sector Corporativo, contamos con tres grandes programas que apoyan al sector empresarial, como son WOMCY Talks, WOMCY Mentoring y WOMCY Talent.

Y, finalmente, para el sector Social, Fundaciones y Organizaciones existen WOMCY Give y WOMCY Back.

Tenemos amplia cobertura y presencia en México, MCA (Multi-Country Area), Brasil y Estados Unidos. Como se mencionó anteriormente, nuestra base se encuentra en Florida, donde reside nuestra presidente, Leticia Gammill, mientras que la Vice Presidencia y liderazgo de MCA, se encuentra en Bogotá, Colombia, liderada por Lizbeth Plaza. Dentro de la organización, se manejan varios liderazgos importantes como son el de México, Brasil, las líderes de WOMCY Marketing LATAM y WOMCY Volunteering LATAM, así como equipos de apoyo, que constituyen un grupo consolidado para los programas que sustentan la organización. Al hablar de la presencia de WOMCY, dentro del panorama mundial, podemos decir con orgullo, que WOMCY, está presente en varios países tales como Estados Unidos, desde el Sur de la Florida, México, Guatemala, El Salvador, Costa Rica, República Dominicana, Colombia, Ecuador, Perú, Bolivia, Chile, Uruguay, Venezuela, Brasil y Argentina, Además, ya tenemos presencia en España con voluntarios y miembros que viven en las Islas Canarias.

Venimos adelantando una serie de Alianzas, con diferentes organizaciones, con las cuales estamos seguros que aportaremos grandes ideas y oportunidades en las áreas de tecnología y educación, con orientación, hacía la Ciberseguridad, para formar las futuras profesionales y especialistas en el área, entre ellos, podemos nombrar a Cisco, fabricante de tecnología y a Frost & Sullivan, empresa consultora que nos permitirá fortalecer el papel de la mujer en el sector de la Ciberseguridad en toda América Latina y el Sur de Florida.

Estamos seguros de que WOMCY, es y será una opción, para muchas jóvenes, en proceso de formación profesional, que necesitan orientación, en las áreas STEAM, es por ello, que en nuestra organización, tenemos personal profesional, preparado para dar mentorías y charlas de orientación, para colegios, universidades y empresas.

CyberSecurity
Información & Privacidad

Donaciones

Contraportada
$500.00

Portada Interior
$450.00

Pagina Interior (Especifica)
$400.00

Pagina Interior
$350.00

Media Página
$200.00

Mas Información

info@csecmagazine.com

LINEAMIENTOS PARA LA PUBLICACIÓN DE ARTÍCULOS

Lineamientos Generales

Los artículos que se publicarán en la revista Cybersecurity – Información y Privacidad- corresponden a:

• Artículos con los resultados de proyectos de investigación que se hayan llevado a cabo.

• Artículos invitados, solicitados directamente al autor, por el Editor o el Comité Editorial.

• Artículos de síntesis y opinión que unifiquen e interpreten el avance del conocimiento en un tema.

• Ensayos y trabajos.

• Resúmenes y acotaciones sobre conferencias, seminarios, talleres y foros.

• En los números especiales de la Revista, patrocinados por un proyecto, podrán publicarse los artículos en idioma inglés.

Las cuales deberán atender los siguientes lineamientos:

1. Deben exhibir coherencia conceptual, profundidad en el dominio de la problemática abordada.

2. Estar escritos en un estilo claro, ágil y estructurado de acuerdo con la naturaleza del texto; con base al modelo APA 6ta. Ed.

3. La extensión mínima del artículo será de 2 páginas con un máximo de 10, formato Word, letra tamaño 12, tipo Arial, interlineado 1.5, márgenes de 3 centímetros, hoja tamaño carta.

4. Los artículos deberán ser entregados en formato digital al correo de la asistente de editores cfa@csecmagazine.com

5. Presentar carta firmada por el autor, según formato anexo, indicar la cobertura temática del artículo de acuerdo con la clasificación según la especialidad.

6. Los manuscritos para su publicación deben incluir:

Título. Debe escribirlo en mayúscula y negrilla, no contener fórmulas ni abreviaturas, ser breve y consistente con el trabajo. En idioma español y en inglés.

Nombre de los autores. Se escribe el primer nombre, la inicial del segundo nombre si lo hay, seguido del apellido. Cuando existe más de un autor, se separan con comas. Se debe indicar con un asterisco la persona a la que puede dirigirse la correspondencia. Además de un extracto del resumen de su experiencia laboral, profesional, adicionando una foto de estudio a color, correo electrónico y redes sociales (LinkedIn)

Nombre de la institución y dirección. Para indicar la afiliación de cada autor use superíndices en el nombre del autor. Para el autor que lleva el asterisco se debe indicar, la dirección completa, teléfono, fax y correo electrónico, a donde pueda dirigirle la correspondencia. Esto solo aplica si representa a una empresa y ha establecido un contrato de publicidad en la revista.

Resumen en español. No debe exceder de 250 palabras. Debe contener los principales resultados y conclusiones haciendo énfasis en los logros alcanzados. Como los resúmenes son copiados directamente de las bases de datos por los interesados, deben contener en forma abreviada el propósito del estudio y las técnicas experimentales, los resultados e interpretaciones de los datos. Los términos relevantes importantes para comprender el contenido del artículo. Se debe entender con facilidad sin tener que recurrir al texto completo.

Introducción. No es necesario incluir toda la literatura sobre el tema en esta sección. Se debe describir el planteamiento general, con la información necesaria en forma concisa, haciendo referencia a los artículos directamente relacionados y que se considere indispensable para el desarrollo del tema y que permita al lector encontrar a otros investigadores del campo, relacionados con el problema o interrogante planteada por el autor. No se deben, por lo tanto, incluir revisiones amplias de la bibliografía.

Materiales y métodos (Opcional): Si existen secciones diferenciadas, deben indicarse con encabezados pertinentes (por ejemplo, síntesis, muestreo, preparación de muestras, etc.). La explicación de los métodos experimentales debe hacerse con los suficientes detalles para que otros investigadores puedan repetirla. La descripción de equipos y reactivos sólo se debe incluir cuando sean específicos o novedosos. Se debe evitar la descripción de procedimientos aplicados con anterioridad por otros autores, pero se debe citar la bibliografía pertinente. Si existen modificaciones a procedimientos ya publicados, se deben incluir los detalles de esta.

Resultados de discusión (Opcional). Presente los resultados en forma clara y concisa, en lo posible en uno de los siguientes formatos: texto, tablas o figuras. Evite duplicar la presentación de los resultados en tablas y figuras. La discusión debe proporcionar una interpretación de los resultados en relación con trabajos previamente publicados y no debe contener repetición considerable o amplia de la sección de resultados o reiteración de lo dicho en la introducción. La información escrita en el texto debe ser citada, pero no se debe repetir en detalle lo ya expuesto. En la discusión es permitida la especulación, pero debe estar bien fundamentada. Dedique al final un párrafo para hacer resaltar las conclusiones más relevantes del trabajo.

Bibliografía. Listado de las fuentes bibliográficas citadas en el artículo en orden alfabético, según el apellido del primer autor, utilizar el modelo APA 6ta. Ed.

CyberSecurity
Información & Privacidad

POR MOTIVOS DE DERECHOS DE AUTOR, ARTICULOS PUBLICADOS EN OTRAS PLATAFORMAS NO SE TOMARÁN EN CUENTA PARA EVITAR TEMAS LEGALES, A MENOS QUE EL AUTOR INDIQUE CLARAMENTE QUE ES PROPIETARIO DE DICHA INVESTIGACION.

La Editorial

cfa@csecmagazine.com

CyberSecurity
Información & Privacidad

Ciudad de Guatemala, de 2,021.

A:

Coordinadora de la Revista Cybersecurity

Presente.

Yo, _____de nacionalidad _____

Identificación No. _____

correo electrónico_____: Teléfono: _____,

Hago constar que el artículo con título:

Acerca de una investigación con el nombre:

Que presento es original y nunca ha sido publicado en otra revista, medio escrito o electrónico y tampoco ha sido presentado a arbitraje en otra revista impresa o digital.

Además, acepto las normas de la revista, en cuanto a procedimiento, formato y demás procedimientos indicados en los lineamientos para publicación de artículos.

_____

Firma

Magazine
CyberSecurity
Información & Privacidad

AUCI invita a participar en la

Convocatoria de Artículos de Ciberseguridad en la

Revista Digital Cybersecurity – Información & Privacidad

(CFA)

Si eres investigador y/o tienes un artículo sobre ciberseguridad de tu autoría, envíanos tu resumen para poder analizarlo y posteriormente publicarlo.

cfa@csecmagazine.com

Magazine

CyberSecurity

Información & Privacidad