Implementación de la ciberseguridad en infraestructuras informáticas

Ricardo Elian Gonzalez[1,3], Eduardo Piray[1,2,3], Miguel Mendez-Garabetti[2,3], Guillermo Romero Arregin[2,3], Santiago Araya[3]

[1] Universidad Empresarial Siglo 21, Decanato de Ciencias Aplicadas. Cordoba, Argentina. eliangonzalez045@gmail.com, epiray@ucaecemdp.edu.ar
[2] Universidad CAECE, Departamento de Sistemas. Mar del Plata, Argentina gromeroarregin@gmail.com, mmendezgarabetti@ucaecemdp.edu.ar
[3] Free and Open Source Software/Hardware Research Laboratory (FOSSHLab). Mendoza, Argentina santiagoaraya913@gmail.com

Resumen La ciberseguridad presenta un amplio espectro de implicancia en la sociedad actual. No obstante, en este articulo permitiremos aportar una explicación y descripción fundamental sobre la implementación de la ciberseguridad en arquitecturas informáticas, la diferenciación de infraestructuras criticas dentro de estas ultimas, la definición de equipos multidisciplinarios que representan la administración de la arquitectura informática y, al final, una especificación de la importancia de concientizar en el cuidado de la ingeniería social utilizada como herramienta de ataques informáticos maliciosos. Es decir, nos enfocamos en reconocer cuales son los recursos que se están utilizando y que conforman a la infraestructura informática, y cuales de estos son los componentes principales dentro del proceso en el cual se este inverso. Esto, permite poder analizar el impacto de la ciberseguridad principalmente por medio de la administración de la arquitectura presente definiendo diversos equipos multidisciplinarios con distintas facultades especificas de la ciberseguridad, protegiendo a la infraestructura, principalmente, del uso de la ingeniería social como un medio para múltiples ataques informáticos, que es el análisis principal al cual nos direccionamos.

Keywords: Ciberseguridad· Infraestructuras informáticas· Infraestructuras criticas· Equipos multidisciplinarios· Ingeniería Social· Ataques informáticos

1. Introducción

En la era digital actual, la ciberseguridad se ha convertido en un pilar fundamental para la protección de las infraestructuras informáticas.
Este artículo explora tres preguntas clave que todo profesional y organización debe considerar:

- ¿Comprendemos realmente el impacto de implementar y gestionar una infraestructura informática con características y propiedades ciberseguras?

- ¿Somos conscientes de la importancia de identificar y proteger las infraestructuras críticas dentro de nuestras arquitecturas informáticas?
- ¿Estamos preparados para enfrentar las amenazas que representa la ingeniería social como herramienta de ataque informático?

A lo largo de las siguientes secciones, abordaremos estas cuestiones fundamentales, proporcionando una visión integral de los desafíos y estrategias en la implementación de la ciberseguridad en entornos informáticos modernos.

2. Infraestructuras criticas envueltas en la arquitectura informática

¿Por que denominamos ciberseguridad y no, por ejemplo, seguridad informática o seguridad de la información?
Por sobre todo, hay que dejar en claro que la ciberseguridad abarca la seguridad del conjunto de recursos informáticos y, tambien, la seguridad del conjunto de información involucrada en los pertinentes escenarios en las cuales se las utilizan tal cual lo describe el NIC Argentina [1][2].
Sin embargo, además de estos conceptos, a continuación la Fig. 1 presenta, a nivel general, una conceptualizacion de las temáticas desprendidas por la ciberseguridad en este articulo:

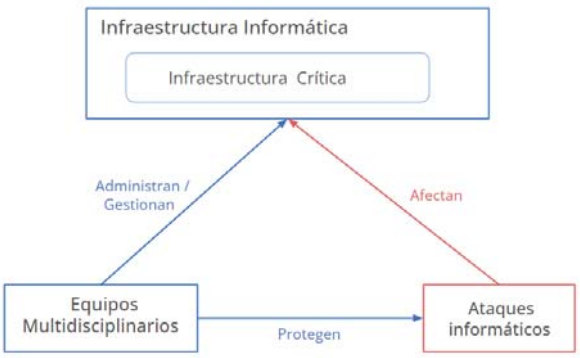

Figura 1. Contexto general. Color azul hace referencia a protección y el color rojo a los ataques que se generan.

Como se puede visualizar, la Fig. 1 expone que al generar una infraestructura informática, es decir, el conjunto de tecnologías utilizadas en distintas situaciones y contextos para fines específicos de forma interna o externa en una organización y/o en otro escenario, se debe tener la perspectiva de identificar internamente a la infraestructura critica, la cual es el conjunto de componentes principales de

la arquitectura que garantizan el central funcionamiento, como lo define Urbina Gabriel P. en la Introduccion a la seguridad informatica, logrando de esta forma, asignar una administración y gestión a los recursos informáticos que estarán encargados de los diversos equipos multidisciplinarios, los cuales protegen a la infraestructura de posibles ataques informáticos, en este caso, por ejemplo, se hace un hincapié en las múltiples amenazas que se realizan mediante el uso de la ingeniería social como herramienta principal [1][3][4].

3. Equipos multidisciplinarios aplicados en el sector de la ciberseguridad

Llegado a este punto, surgen mas preguntas, por ejemplo; ¿como se gestiona o administra la arquitectura informática y su infraestructura critica interna aplicando características y propiedades ciberseguras?
Pues, para poder realizar una administración de una arquitectura informática, sea del tipo que sea, hay que tener en cuenta la gestión de diversos equipos multidisciplinarios que se encargan de trabajar en diversas tareas abocadas a distintas sub-áreas en el mismo sector de la ciberseguridad [5].
A continuación, se presenta la Fig. 2 la cual enmarca lo descrito, dejando en claro, por un lado, a los diversos equipos pertinentemente involucrados en el sector de la ciberseguridad y, por otra parte, resumidamente, cual es el aspecto que abarcan en sus respectivas tareas:

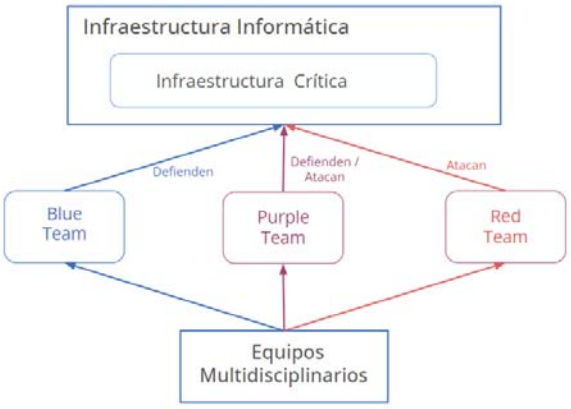

Figura 2. Equipos multidisciplinarios aplicados en la ciberseguridad

En la Fig. 2 se puede apreciar como, primeramente, el blue team se encarga de analizar constantemente la mejor perspectiva de defensa para proteger la arquitectura informática de ataques maliciosos. Esto, con ayuda de las técnicas

de ataque implementadas por los equipos de red team para poder encontrar y exponer vulnerabilidades en la infraestructura.
A su vez, también, se involucra el soporte de ataque y defensa simultáneamente que brindan los equipos de purple team, ya que estos generan un análisis de todo lo expuesto rodeado a la protección y búsqueda de mejoras de ciberseguridad en la arquitectura [6].
Entonces, por ejemplo, el equipo de blue team se basa en analizar las propiedades de protección impuestas en la arquitectura en el contexto en el cual se este inverso. Pero, el equipo de red team, teniendo en cuenta la infraestructura, evalúa implementar sobrecargas de ataques informáticos analizando el impacto y respuesta a los mismos. Es por ello, que en base a estas dos implicaciones de estos equipos, el equipo de purple team analiza como lo experimentado por el red team permite mejorar la protección de la infraestructura. Y, a su vez, como lo realizo por el blue team permite plasmar técnicas de ataque en los cuales se busquen explotar muchas mas vulnerabilidades.

4. El impacto de la Ingeniería Social como herramienta de ataque maliciosa

Teniendo en cuenta todo lo definido hasta este momento, ¿cual es el impacto de la ingeniería social como herramienta para realizar ataques informaticos maliciosos?
La ingeniería social es una de las herramientas mas usadas para desencadenar todo tipo de ataques que violen la ciberseguridad en diversos contextos a nivel general. Mediante esta, se puede realizar engaños a los seres humanos y generar un control de situación que, por medio de la tecnología, se permite extraer provecho para diferentes fines, por ejemplo, robo de dinero, obtención de información critica de organizaciones y/o personas especificas.
Una de las formas de poder utilizar la ingeniería social con fines maliciosos es por medio del denominado Phishing. Justamente este, permite a los atacantes engañar a las personas, usuarias de un sistema en particular, por medio de diversos recursos tecnológicos creados que son falsos con el fin de poder robar y extraer información sensible, contraseñas de otros sistemas involucrados, dinero, números de tarjeta de crédito, entre muchas otras cuestiones particulares [7]

No obstante, el Phising no es la única muestra de lo que se puede realizar con la ingeniería social de forma maliciosa. Este, es uno de los tantos ataques y formas con las cuales puede variar el uso de la ingeniería social convirtiéndola en una amenaza, por ejemplo, para las infraestructuras informáticas, pero, también, hacia la integridad de las personas y su información administrada.

5. Conclusiones y trabajo que representa el futuro

Por sobre todo, destacar que la ingeniería social es uno de los mayores medios de multíplices ataques maliciosos dentro de los tantos que se presentan actual-

mente. Es por esto que decidimos enfocarnos principalmente en esta temática y, con esto, permitir destacar la implicancia en la gestión de tanto infraestructura informática como critica que realizan los equipos de blue team, red team y purple team. Esto quiere decir que, a futuro, existe un proceso amplio para poder realizar análisis de protección de las arquitecturas como lo realiza el blue team, implementando diversas técnicas de tipo red team y evaluando como estas dos áreas de la ciberseguridad se equilibran para cumplir con características relacionadas a purple team representando un mayor avance en la evolución tecnológica presente.

Para concluir, es muy relevante destacar que este artículo surge de un proyecto de investigación en curso, respaldado por la Universidad Empresarial Siglo 21, la Universidad CAECE y el Laboratorio de Investigación en Software y Hardware Libre (FOSSHLab), bajo la dirección del Dr. Miguel Méndez-Garabetti y el Ing. Eduardo Piray.
Este proyecto se centra en el estudio de técnicas de identidad digital de usuarios, analizando la transición de la web 2.0 a la web 3.0 en el contexto de la ciberseguridad.Y, por otra parte, la exploración de tecnologías emergentes como la Inteligencia Artificial (IA) y la Blockchain, y su aplicación en el ámbito de la ciberseguridad, subrayando principalmente. la importancia de la evolución constante en las estrategias de ciberseguridad, adaptándose a las nuevas tecnologías y desafíos en el entorno digital.

Referencias

1. Gabriel B. Urbina. Introducción a la Seguridad Informática.
2. Argentina NIC. ¿Qué es Ciberseguridad?
3. Verónica P. Tintín-Perdomo, José R. Caiza-Caizabuano, and Fernando S. Caicedo-Altamirano. Arquitectura de redes de información. Principios y conceptos. *Dominio de las Ciencias*, 4(2):103, April 2018.
4. Francisco P. Téllez. Ciberseguridad en Infraestructuras Criticas.
5. Vicente Pons Gamon. Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, (20):80, June 2017.
6. Oscar E. Ramírez Álvarez. Capacidades tecnicas, legales y de gestion para equipos blue team y red team.
7. Eduardo Benavides, Walter Fuertes, and Sandra Sanchez. Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencia y Tecnología*, 13(1):97–104, June 2020.