REVISTA MULTIDISCIPLINARIA
DESARROLLO AGROPECUARIO, TECNOLOGICO, EMPRESARIAL Y HUMANISTA
UNIVERSIDAD TECNICA DE COTOPAXI - LA MANA. COTOPAXI. ECUADOR
ISSN: 2773-7527
Volumen 6. No. 1
mayo 2024

Seguridad, amenazas y mecanismos de protección de los dispositivos móviles

Security, threats and protection mechanisms for mobile devices

Javier Guaña Moya[1]

[1]Instituto Superior Universitario Japón, Quito – Ecuador

Correo de correspondencia: eguana@itsjapon.edu.ec

Información del artículo

Tipo de artículo: *Artículo original*

Recibido: *15/10/2023*

Aceptado: *15/03/2024*

Publicado: *06/05/2024*

Revista: *DATEH*

Resumen

En la actualidad más de la mitad de los equipos de computación comerciales son móviles, presentando estos dispositivos diversos y constantes desafíos para la seguridad de la red, destacando que la configuración WiFi desconocida, aceptación de aplicaciones no identificadas, conexión a sitios que no son de confianza y la descarga de aplicaciones de dichos sitios pueden enumerarse como los principales problemas que se presentan al emplear dispositivos móviles. Por esta razón es de vital importancia que los usuarios conozcan las diversas amenazas de seguridad que ponen en riesgo datos e información contenida en los dispositivos móviles, los tipos y los principales sistemas de protección desarrollados en la actualidad con el fin de evitar pérdidas o robo de información y documentos privados personales y empresariales que pueden poner en riesgo la integridad y seguridad de los usuarios y las organizaciones. El objetivo de la investigación es identificar las diversas amenazas de seguridad que ponen en riesgo datos e información contenida en los dispositivos móviles, estableciendo los tipos de amenazas, revisando las distintas estrategias para evitarlas y describiendo los principales sistemas de protección desarrollados en la actualidad.

Palabras clave: *Dispositivos móviles, seguridad, red móvil, protección.*

Abstract

Currently, more than half of commercial computing equipment is mobile, presenting these devices with diverse and constant challenges for network security, highlighting that unknown WiFi configuration, acceptance of unidentified applications, connection to sites that are not Trust and downloading apps from such sites can be listed as the top issues when using mobile devices. For this reason, it is of vital importance that users know the various security threats that put data and information contained in mobile devices at risk, the types and the main protection systems currently developed in order to avoid loss or theft of data. private personal and business information and documents that can put the integrity and security of users and organizations at risk. The objective of the research is to identify the various security threats that put data and information contained in mobile devices at risk, establishing the types of threats, reviewing the different strategies to avoid them and describing the main protection systems currently developed.

Keywords: *Mobile devices, security, mobile network, protection.*

Forma sugerida de citar (APA): López-Rodríguez, C. E., Sotelo-Muñoz, J. K., Muñoz-Venegas, I. J. y López-Aguas, N. F. (2024). Análisis de la multidimensionalidad del brand equity para el sector bancario: un estudio en la generación Z. Retos Revista de Ciencias de la Administración y Economía, 14(27), 9-20. https://doi.org/10.17163/ret.n27.2024.01.

INTRODUCCIÓN

El uso de dispositivos móviles está en creciente aumento a medida que los individuos los emplean principalmente para comunicarse, además de crear y editar documentos, almacenar y recuperar archivos de datos y navegar por Internet, mientras que en el caso de las organizaciones los dispositivos móviles incrementan la agilidad de los empleados, permitiendo el trabajo de forma remota (Guevara, 2018). Sin embargo, la omnipresencia y evolución de estos dispositivos crea una amenaza especial debido que las políticas y los controles para las computadoras no son lo suficientemente amplios para cubrir las nuevas amenazas que plantean estos dispositivos, los cuales han facilitado que los piratas

ISSN: 2773-7527
Volumen 6. No. 1
Mayo 2024

informáticos exploten los sistemas, aumentando de esta manera la posibilidad de comprometer archivos confidenciales (Leal, 2019). Es por ello que la mayoría de las empresas fabricantes de dispositivos móviles han tratado de abordar estos problemas de seguridad creado controles específicos para reducir la probabilidad de delitos informáticos (Kearns, 2016).

Por otra parte, es evidente que la mayoría de los equipos de computación empleados por las empresas son móviles, presentando el aumento de los dispositivos de Internet de las cosas (IoT) nuevos desafíos para la seguridad de red y como consecuencia, los equipos de tecnología de la información (TI) deben adaptar constantemente las estrategias de seguridad, considerando que en los planes de seguridad de redes se debe tener en cuenta todas las ubicaciones y los diversos usos que los empleados exigen de la red empresarial y, al mismo tiempo, cada usuario debe realizar algunos pasos simples para mejorar la seguridad de los dispositivos móviles (Cisco, 2020).

En base a esto se desarrolla la presente revisión bibliográfica con el objetivo de establecer las diversas amenazas de seguridad que ponen en riesgo datos e información contenida en los dispositivos móviles, estableciendo los tipos, revisando las distintas estrategias para evitarlas y describiendo los principales sistemas de protección desarrollados en la actualidad.

MATERIALES Y MÉTODOS

La presente investigación se desarrolló en base a la normativa de revisión sistemática de la literatura establecida por Kitchenham (Kitchenham, 2004), con el fin de obtener información relacionada con las preguntas de investigación que se plantean para el desarrollo de la misma. Esta normativa establece las siguientes etapas:

- Planificación de la revisión
- Realización de la revisión
- Análisis de resultados.

a) Planificación de la revisión

El objetivo de la investigación es identificar las diversas amenazas de seguridad que ponen en riesgo datos e información contenida en los dispositivos móviles, estableciendo los tipos de amenazas, revisando las distintas estrategias para evitarlas y describiendo los principales sistemas de protección desarrollados en la actualidad.

Para el desarrollo del tema se plantearon las siguientes preguntas de investigación:
P1: ¿Qué es la seguridad de los dispositivos móviles?
P2: ¿Cuáles son los tipos de amenazas de la seguridad móvil?
P3: ¿Cuáles son los mecanismos de protección de los dispositivos móviles en la actualidad?

Se accedió a la información proporcionada por bases de datos digitales, tal como ACM Digital Library, IEEE eXplorer, Science Direct Elsevier, Scopus y Springer Link, referente a temas relacionados con la red móvil, seguridad de los dispositivos móviles, estrategias de prevención y protección contra amenazas a sistemas móviles, identificando entre las fuentes de información encontradas revistas académicas y publicaciones técnicas, comprendidas entre los años 2015 y 2022, con una estrategia de búsqueda fundamentada en aspectos relacionados con las preguntas de investigación.

Los criterios de inclusión que se consideraron en la selección de documentos son: artículos que abordan la seguridad de los dispositivos móviles en cualquiera de sus modalidades, mecanismos de prevención contra amenazas a la red móvil y artículos de casos de aplicación de estrategias de protección. Mientras que como criterios de exclusión se consideró información publicada en sitios web generales, documentos con aportes irrelevantes y blogs.

b) Realización de la revisión

En esta fase se seleccionaron los artículos en base a los criterios de inclusión y exclusión, revisando los títulos de los artículos, contenido y conclusiones con el fin de determinar el aporte a las preguntas planteadas.
Como resultado de la búsqueda se identificaron 67 documentos, de los cuales se seleccionaron 37 que cumplieron con los criterios establecidos.

RESULTADOS Y DISCUSIÓN

Entender a qué se refiere cuando se habla acerca de la seguridad de los dispositivos móviles fue posible al obtener respuestas de la P1: ¿Qué es la seguridad de los dispositivos móviles?

La seguridad de dispositivos móviles se refiere a las medidas diseñadas para proteger la información confidencial almacenada y transmitida por computadoras portátiles, teléfonos inteligentes, tabletas, dispositivos portátiles y otros equipos móviles. Estas estrategias tienen como principal objetivo evitar que usuarios no autorizados accedan a la red de las organizaciones, representando un aspecto completo de los planes de seguridad empresarial (Avizienis et al., 2004; VMware, 2022).

Actualmente más de la mitad de los equipos de computación comerciales son dispositivos móviles, presentando estos diferentes y constantes desafíos para la seguridad de las redes, seguridad que debe estar fundamentada en todas las ubicaciones y usos que los

ISSN: 2773-7527
Volumen 6. No. 1
Mayo 2024

empleados requieren de las redes empresariales. Estas amenazas potenciales para los dispositivos incluyen aplicaciones móviles maliciosas, estafas de phishing, fuga de datos, redes WiFi poco confiables y spyware. Adicionalmente, las organizaciones deben considerar la posibilidad de que un empleado pierda un dispositivo móvil o se lo roben. Por tanto, con la finalidad de evitar una brecha de seguridad deben tomarse medidas preventivas claras para reducir el riesgo (Yamin & Katt, 2019).

P2: ¿Cuáles son los tipos de amenazas de la seguridad móvil?

Las amenazas de seguridad móvil generalmente son consideradas como una única amenaza que engloba todo; sin embargo, en la práctica existen cuatro tipos de amenazas de seguridad móvil de las que las organizaciones deben tomar medidas para protegerse, siendo estas las siguientes:

Amenazas a la seguridad de las aplicaciones móviles: Este tipo de amenazas se basan en aplicaciones, es decir, ocurren cuando las personas descargan aplicaciones que parecen legítimas, pero en realidad extraen datos del dispositivo, tal como el spyware y el malware que roban información personal y comercial sin que las personas se den cuenta de lo que está sucediendo (Gontovnikas, 2021). De acuerdo a datos extraídos del informe de Seguridad Móvil de Check Point (Prensario, 2021) en el 2020 el 46% de las organizaciones sufrió amenazas de red debido a descargas de aplicaciones móvil maliciosas, indicando además que cuatro de cada diez equipos móviles son vulnerables.

Amenazas de seguridad móvil basadas en la web: Las amenazas basadas en la web son sutiles y por lo general pasan desapercibidas. Ocurren cuando las personas visitan sitios afectados que parecen estar bien en el front-end pero, en realidad, descargan automáticamente contenido malicioso en los dispositivos (Q. Li & Clark, 2013).

Amenazas a la seguridad de la red móvil: Las amenazas basadas en la red son especialmente comunes y riesgosas porque los ciberdelincuentes pueden robar datos sin cifrar mientras las personas usan redes WiFi públicas (Yesilyurt & Yalman, 2016). Existen grupos conocidos como APT (Advanced Persistent Threat) que evaden las herramientas de seguridad tradicionales de manera sofisticada mediante ciberataques selectivos con la finalidad de espiar a los usuarios y obtener datos confidenciales, estos grupos poseen como principal objetivo los teléfonos móviles (Prensario, 2021).

Amenazas a la seguridad de los dispositivos móviles: Las amenazas físicas a los dispositivos móviles comúnmente se refieren a la pérdida o robo de un dispositivo. En estos casos los piratas informáticos tienen acceso directo al hardware donde se almacenan los datos privados, esta amenaza es especialmente peligrosa para las empresas. Según datos de ESET, empresa de seguridad informática, el 58% de los usuarios de equipos móviles en Latinoamérica ha sido víctima de robo, señalando que a medida que crece el uso de dispositivos inteligentes también se incrementa considerablemente el robo de los mismos (Siliconweek.com, 2022).

Entre los ejemplos más comunes de estas amenazas y las estrategias empleadas para evitarlas, se pueden mencionar los siguientes:

Ingeniería social: Este tipo de ataques suceden cuando los ciberdelincuentes envían correos electrónicos falsos (phishing) o mensajes de texto (smishing) con la finalidad de engañar a los usuarios para que entreguen información privada como contraseñas o descarguen malware en los dispositivos. De acuerdo a informes de seguridad cibernética, publicados por Lookout y Verizon (Shires, 2022), los ataques de phishing a móviles empresariales aumentaron un 37%, siendo estos la principal causa de filtraciones de datos a nivel mundial en 2020.
La mejor defensa contra el phishing y otros ataques de ingeniería social es educar a los empleados en cómo detectar correos electrónicos y mensajes SMS que parezcan sospechosos para evitar ser víctimas de ellos por completo. También la reducción de la cantidad de personas que tienen acceso a datos o sistemas confidenciales puede ayudar a proteger a las organizaciones como consecuencia de la menor cantidad de puntos de acceso que los atacantes tienen disponible para obtener acceso a sistemas o información críticos (Kumar et al., 2020).

Fuga de datos por medio de aplicaciones maliciosas: Las organizaciones constantemente se enfrentan a una amenaza creciente por los millones de aplicaciones disponibles, en su mayoría en los dispositivos de usuarios y empleados, más que por el malware móvil en sí mismo. Se considera que el 85% de las aplicaciones móviles actuales no son seguras en gran medida, esta circunstancia favorece que los piratas informáticos encuentren fácilmente una aplicación móvil desprotegida y la usen para diseñar ataques más grandes o robar datos, billeteras digitales, detalles de back-end y otros tipos de fraudes directamente desde la aplicación (Rajagopal & Ramesh, 2016).

Se puede mencionar como ejemplo los casos en que el usuario visita Google Play o App Store para descargar

ISSN: 2773-7527
Volumen 6. No. 1
Mayo 2024

aplicaciones que parecen lo suficientemente inofensivas, para el proceso de descarga estas apps solicitan una serie de permisos previos, permisos que generalmente requieren algún tipo de acceso a archivos o carpetas en el dispositivo móvil, en estos casos la mayor parte de las personas solo miran la lista de permisos y aceptan sin revisarlos en detalle (Stair & Reynolds, 2020). Esta falta de escrutinio incrementa la vulnerabilidad de los dispositivos y de los datos personales u organizacionales; independientemente que la aplicación funcione de manera correcta, aún tiene el potencial de extraer datos corporativos y enviarlos a un tercero, como puede ser un competidor, exponiendo de esta manera información confidencial de productos o negocios.

La manera más efectiva de proteger datos sensibles personas u organizacionales contra la fuga de datos a través de aplicaciones maliciosas o no seguras es empleando herramientas de administración de aplicaciones móviles (MAM). Estas herramientas permiten a los administradores de TI administrar las aplicaciones corporativas, bien sea borrando o controlando los permisos de acceso en los dispositivos de los empleados sin interrumpir las aplicaciones o los datos personales de los empleados (Hole, 2015; Steele, 2020).

WiFi público no seguro

Las redes WiFi públicas generalmente son menos seguras que las redes privadas porque no hay forma de saber quién configuró la red, cómo está protegida con encriptación o quién está accediendo o monitoreando en tiempo real. Por otra parte, en la medida que más empresas ofrecen opciones de trabajo remoto, las redes WiFi públicas usadas por los empleados para acceder a los servidores representan riesgos elevados para las organizaciones (Sombatruang et al., 2018).

En otros casos los ciberdelincuentes configuran redes WiFi similares a las reales, sin embargo, constituyen una fachada para capturar los datos que pasan a través del sistema. La creación de puntos de acceso WiFi falsos en espacios públicos con nombres de red que parecen completamente legítimos es extremadamente sencillo, razón por la cual los usuarios se conectan con total confianza. Por lo tanto, la mejor manera de proteger a las organizaciones contra las amenazas a través de redes WiFi públicas es educar a los usuarios a utilizar una red privada virtual (VPN) específica para acceder a los sistemas o archivos de la empresa, esta precaución garantizará que la sesión se mantenga privada y segura, incluso si utilizan una red pública para acceder a los sistemas (Sobh, 2013).

Brechas de cifrado de extremo a extremo

El cifrado de datos es el proceso que, mediante un algoritmo, transforma los caracteres de texto estándar en un formato ilegible, para lograr esto se emplean claves de cifrado que codifican los datos de modo que solamente los usuarios autorizados puedan leerlos. En el caso del cifrado de extremo a extremo se utiliza un procedimiento similar, sin embargo, va un poco más allá al asegurar las comunicaciones desde el origen hasta el receptor (IBM, 2020).

Las redes WiFi públicas sin cifrar son uno de los ejemplos más comunes de una brecha de cifrado, representando un gran riesgo para las organizaciones. Al no estar protegida la red se origina una abertura en la conexión para que los ciberdelincuentes accedan a la información que los usuarios y empleados comparten entre los dispositivos móviles y los sistemas. Sin embargo, las redes WiFi no son lo único que representa una amenaza, cualquier aplicación o servicio que no esté cifrado puede proporcionar a los ciberdelincuentes acceso a información confidencial de la empresa, así como también cualquier aplicación de mensajería móvil sin cifrar que utilicen los empleados para discutir información de trabajo, todos estos casos representan un punto de acceso para diseñar un fraude (Vandenberg, 2017).

La mejor solución para evitar esta amenaza es asegurar que todo esté cifrado, considerando que para cualquier información confidencial el cifrado de extremo a extremo es fundamental. Esto incluye asegurar que los proveedores de servicios con los que trabajan las organizaciones cifren sus servicios para evitar el acceso no autorizado, así como el confirmar que, tanto los dispositivos de los usuarios como los sistemas, estén codificados (Ulloa Hallo, 2021).

Dispositivos de Internet de las Cosas (IoT)

Los tipos de dispositivos móviles que acceden a los sistemas de la organización se están ramificando desde teléfonos móviles y tabletas, incluyendo tecnología portátil y dispositivos físicos. Muchos de los últimos dispositivos móviles de IoT tienen direcciones IP, lo que permite a los ciberdelincuentes usarlas para obtener acceso a la red personal o de las organizaciones por medio de Internet, especialmente si esos dispositivos están conectados a los sistemas de red (Yadav & Prasad, 2019). Existe una gran cantidad de dispositivos IoT conectados a las redes, superior a lo que se cree, de acuerdo a un estudio de Infoblox el 78% de los líderes de TI de cuatro países diferentes reportaron que más de mil dispositivos IoT en la sombra accedían a las redes diariamente(Infoblox, 2021). Las herramientas de administración de dispositivos móviles (MDM) también pueden ayudar a combatir las amenazas ocultas de IoT, así como las herramientas de administración de identidad y acceso (IAM). Sin embargo, la seguridad de IoT/Machine-to-Machine (M2M) todavía se encuentra en una fase primaria, por lo tanto, depende de cada organización implementar las normas técnicas y

ISSN: 2773-7527
Volumen 6. No. 1
Mayo 2024

políticas adecuadas para garantizar que los sistemas sean seguros (Infoblox, 2021).

Software espía
El spyware se utiliza para encuestar o recopilar datos y se instala con mayor frecuencia en un dispositivo móvil cuando los usuarios hacen clic en un anuncio o publicidad maliciosa, así como también mediante estafas que engañan a los usuarios a que realicen descargas de manera inconsciente. Los dispositivos móviles son objetivos perfectos para la extracción de datos con software espía, lo que incluye datos corporativos privados si estos dispositivos están conectado a sus sistemas (Salih & Mohammed, 2020).

Las aplicaciones de seguridad móvil dedicadas, tal como Play Protect de Google, pueden ayudar a los usuarios a detectar y eliminar el spyware que intente instalarse en los dispositivos para acceder a los datos de la empresa (Schmitt, 2022). Una manera de evitar esta amenaza es asegurar que los empleados mantengan actualizados tanto los sistemas operativos como las aplicaciones de los equipos móviles, lo que garantiza que los dispositivos y los datos se mantengan protegidos contra las últimas amenazas de spyware.

Malos hábitos de contraseña
Un estudio desarrollado por Balbix en 2020 (Balbix Inc., 2020) señala que el 99% de las personas encuestadas reutilizaron sus contraseñas entre cuentas de trabajo o entre cuentas de trabajo y personales, también indica que en promedio cada contraseña de usuario se comparte en 2,7 cuentas, considerando además que las contraseñas que los usuarios reutilizan generalmente son débiles al incluir nombres o la fecha de nacimiento.

Estas infracciones causadas por credenciales comprometidas no son el resultado de una pequeña minoría de usuarios con mala higiene de contraseñas, en realidad son el resultado de un problema generalizado. Se ha determinado que los problemas relacionados con las contraseñas clave más responsables del riesgo general de incumplimiento para las organizaciones son las siguientes:

- Contraseñas de sistema débiles y predeterminadas en controladores de dominio y otros componentes y servicios de infraestructura.
- Credenciales almacenadas en caché para iniciar sesión en sistemas de misión crítica.
- Máquinas de usuarios privilegiados con una alta probabilidad de incumplimiento al iniciar sesión en servidores centrales.
- Reutilización de contraseñas entre cuentas laborales y personales.

Estos comportamientos brindan grandes oportunidades para ataques cibernéticos de fuerza bruta basados en credenciales, como el relleno de credenciales o el rociado de contraseñas, porque los ciberdelincuentes pueden usar credenciales débiles o robadas para acceder a datos confidenciales a través de las aplicaciones móviles de la empresa.

P3: ¿Cuáles son los mecanismos de protección de los dispositivos móviles en la actualidad?

Los requisitos básicos de ciberseguridad siguen siendo los mismos tanto para los dispositivos móviles como para las computadoras no móviles, siempre enfocados en mantener y proteger la confidencialidad, la integridad y la identidad. Sin embargo, las tendencias actuales de seguridad móvil han originado nuevas oportunidades y desafíos, lo que requiere el planteamiento de la redefinición de la seguridad para los dispositivos informáticos personales. Por ejemplo, las capacidades y expectativas varían de acuerdo al factor de forma y tamaño del dispositivo, los avances en las tecnologías de seguridad, las tácticas de amenazas en rápida evolución y la interacción del dispositivo, como el tacto, el audio y el video (IBM, 2021a).

En base a lo anterior las organizaciones de TI y los equipos de seguridad deben comenzar a reconsiderar cómo lograr los requisitos de seguridad a la luz de las capacidades de los dispositivos, el panorama de amenazas móviles y las expectativas cambiantes de los usuarios. Es decir, estos profesionales necesitan proteger múltiples vulnerabilidades dentro del entorno dinámico y de crecimiento masivo de dispositivos móviles, ofreciendo un entorno móvil seguro protección en seis áreas principales: gestión de la movilidad empresarial, seguridad del correo electrónico, protección de terminales, VPN, puertas de enlace seguras y agente de acceso a la nube.

Gestión de la movilidad empresarial (EMM)
Representa el conjunto de herramientas y tecnologías que mantienen y administran la manera cómo se utilizan los dispositivos móviles y de mano dentro de una organización para las operaciones comerciales de rutina, combinando la gestión de usuarios, aplicaciones y contenido con una sólida seguridad de datos para ayudar a los usuarios a conectarse rápidamente a los recursos corporativos. Una solución EMM robusta simplifica la administración y configuración de dispositivos, ayuda a iniciar solicitudes de registro, distribuye aplicaciones, documentos y permite una mayor colaboración. En la actual situación de incremento de los trabajos remotos los EMM convencionales deben estar diseñados para brindar a los usuarios un acceso fluido a los sitios de la intranet y usar las capacidades de VPN de sus dispositivos para

ISSN: 2773-7527
Volumen 6. No. 1
Mayo 2024

acceder a aplicaciones y datos corporativos con facilidad y velocidad (IBM, 2021b).

La efectividad de EMM se evidencia en la investigación desarrollada por Camacho Hernández (Camacho Hernández, 2015) con el fin de mejorar la seguridad en la prestación del servicio de correo electrónico corporativo en dispositivos móviles dentro de una institución pública, aplicando políticas y herramientas de EMM, donde concluyen que al identificar los requerimientos relacionados con el uso del correo electrónico corporativo en dispositivos móviles, así como las vulnerabilidades y amenazas en la utilización de este servicio estas herramientas permitieron a los usuarios utilizar el servicio de correo electrónico de forma transparente y segura en cada dispositivo.

Seguridad del correo electrónico

Los emails son utilizados de forma universal por empresas, agencias gubernamentales y usuarios individuales, en consecuencia, por necesidad, los usuarios confían en que los sistemas de correo electrónico se mantengan seguros y protegidos. Sin embargo, estos sistemas suelen ser complejos y las pruebas exhaustivas son casi imposibles, resultando que con mucha frecuencia contengan errores y vulnerabilidades de seguridad. Por lo tanto, para proteger los datos de las amenazas cibernéticas basadas en el correo electrónico, como el malware, el robo de identidad y las estafas de phishing, las organizaciones deben monitorear el tráfico de correo electrónico de manera proactiva, incluyendo también servicios de antivirus, antispam, control de imágenes y control de contenido, como mecanismos de protección adecuada del correo electrónico (T. Li et al., 2017).

Protección de punto final

Con el vertiginoso desarrollo tecnológico, tal como la tecnología móvil, IoT y la nube, las organizaciones conectan puntos finales nuevos y diferentes a su entorno de respuesta, por lo que la seguridad de puntos finales incluye protección antivirus, prevención de pérdida de datos, cifrado y gestión de seguridad de puntos finales, lo cual ha favorecido el surgimiento de un mercado importante para varios productos de software que brindan protección de datos de punto final para las organizaciones (Chandel et al., 2019).

Describe Cando Estrella (Cando Estrella, 2020) en su estudio que la implementación de una plataforma de seguridad para mitigar las amenazas informáticas y brindar protección a la información que se maneja dentro de la organización administrando los dispositivos de punto final establece una barrera de protección para los dispositivos finales en donde se almacena información valiosa empleada dentro de las instituciones, logrando de esta manera garantizar la disponibilidad, confidencialidad e integridad de la misma.

VPN

La red privada virtual (VPN) representa el enfoque tradicional para mantener una conexión segura de extremo a extremo entre dos puntos finales, lo que permite a las organizaciones ampliar de forma segura su intranet privada sobre el marco existente de una red pública como Internet. Con una VPN, una empresa puede controlar el tráfico de la red al mismo tiempo que proporciona funciones de seguridad esenciales, como la autenticación y la privacidad de los datos (Alshalan et al., 2016).

El estudio aplicado de León Gómez (León Gómez, 2018) afirma que al monitorear el rendimiento en la implementación de una Red Privada Virtual (VPN) se comprobó el fortalecimiento de la seguridad al prevenir ataques de personas ajenas a la red dirigidos a la información que viaja a través de ella y a situaciones que ponen en riesgo la integridad de la información, además de generar problemas de rendimiento en la propia VPN.

Puertas de enlace seguras

Una puerta de enlace segura es una conexión de red protegida que conecta cualquier cosa con cualquier cosa. Hace cumplir políticas coherentes de seguridad y cumplimiento de Internet para todos los usuarios, independientemente de la ubicación o el tipo de dispositivo utilizado, manteniendo el tráfico no autorizado fuera de la red de la organización (Gupta et al., 2014). Es por ello que, basado en este sistema, Bienhaus et al. (Bienhaus et al., 2021) propusieron una arquitectura de seguridad para una puerta de enlace que conecta sensores y componentes de automatización de líneas de ensamblaje con Internet o sistemas basados en la nube, utilizando un módulo de plataforma segura para proteger las claves criptográficas utilizadas en los protocolos de comunicación segura y brindar protección contra la manipulación ilegítima del firmware.

Agente de acceso a la nube (CASB)

Un CASB es un punto de cumplimiento de políticas entre usuarios y proveedores de servicios en la nube (CSP). Este supervisa la actividad relacionada con la nube y aplica reglas de seguridad, cumplimiento y gobernanza en torno al uso de recursos basados en la nube. Por tanto, el control de acceso posee una importancia primordial al garantizar diversos servicios de seguridad, tales como autenticación, identificación, confidencialidad e integridad (Yahya et al., 2016).

De acuerdo a Agrawal y Tapaswi (Agrawal & Tapaswi, 2019) para fortalecer la seguridad de los protocolos de control de acceso para el entorno de nube móvil se utilizan

ISSN: 2773-7527
Volumen 6. No. 1
Mayo 2024

atributos dinámicos de dispositivos móviles, sin embargo, el problema de la debilidad o la desconexión de la red móvil es una tarea crítica a tratar. Es por ello que diseñaron un sistema de control de acceso y confidencialidad de los datos mediante el cifrado de atributos dinámicos, empleando las parejas de agentes móviles para tratar el tema de la conexión a la red y una clave secreta distribuida mediante un protocolo de emisión de claves anónimas con el fin de preservar el anonimato del usuario, evitando así que sean perfilados por los ciberdelincuentes, proporcionando este enfoque una comunicación ininterrumpida y segura entre los clientes y el servidor de almacenamiento en la nube

CONCLUSIONES

Es bastante complicado generar una estructura de seguridad común que aborde todas las vulnerabilidades en el mundo de los dispositivos móviles, por lo que es muy poco probable que surja una solución única que resuelva todos los problemas potenciales. En primer lugar, los operadores de las redes, especialmente inalámbricas, deben asumir la responsabilidad de proporcionar un mecanismo de comunicación seguro y eficiente, abarcando estos canales de comunicación procedimientos de autenticación sólidos que garanticen la seguridad de los dispositivos móviles y, en segundo lugar, los propios dispositivos móviles deben incorporar seguridad a nivel de sistema para garantizar que no sean susceptibles a ataques tanto en formato de red como de virus.

Los fabricantes de aplicaciones y servicios para dispositivos móviles deben incorporar y actualizar constantemente sólidos procedimientos de autenticación, autorización y contabilidad y, sin embargo, implementando todos estos mecanismos los problemas adicionales que deben atenderse con el fin de garantizar que los dispositivos móviles sean seguros son las preocupaciones políticas y culturales, la ingeniería social, las prácticas y políticas comerciales.

En conclusión, no existe un dispositivo que sea totalmente seguro, por lo que los usuarios deben conocer y aplicar las estrategias para evitar cualquier tipo de fraudes cibernéticos, mientras que los fabricantes de redes y dispositivos deben esforzarse permanentemente en brindar seguridad y protección a los usuarios.

REFERENCIAS BIBLIOGRÁFICAS

Guevara, A. (2018). Dispositivos Móviles. Seguridad, (7). Recuperado el 18 de agosto de 2022, de https://revista.seguridad.unam.mx/numero-07/dispositivos-moviles

Kearns, G. (2016). Countering Mobile Device Threats: A Mobile Device Security Model. Journal of Forensic & Investigative Accounting, 8(1), 36-48.

Cisco. (2020). ¿Qué es la seguridad de dispositivos móviles? Recuperado el 5 de mayo de 2022, de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/security/mobile-device-security.html

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. Keele, UK: Keele Univ. Recuperado el 5 de mayo de 2022, de https://www.researchgate.net/publication/228756057_Procedures_for_Performing_Systematic_Reviews

Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, 1(1), 11-33. https://doi.org/10.1109/TDSC.2004.2

Yamin, M. M., & Katt, B. (2019). Mobile device management (MDM) technologies, issues and challenges. En Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (pp. 143-147). doi: 10.1145/3309074.3309103

Gontovnikas, M. (2021). Las 9 amenazas de seguridad más comunes para dispositivos móviles en 2021. Recuperado el 5 de mayo de 2022, de https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021/

Li, Q., & Clark, G. (2013). Mobile Security: A Look Ahead. IEEE Security & Privacy, 11(1), 78-81. https://doi.org/10.1109/MSP.2013.15

Yesilyurt, M., & Yalman, Y. (2016). Security Threats on Mobile Devices and their Effects: Estimations for the Future. International Journal of Security and Its Applications, 10(2), 13-26. https://doi.org/10.14257/ijsia.2016.10.2.02

Siliconweek.com. (2022). El robo de celulares en América Latina: un problema aún por resolver. Recuperado el 6 de mayo de 2022, de https://www.siliconweek.com/e-enterprise/el-robo-de-celulares-en-america-latina-un-problema-aun-por-resolver-55123?print=print

Shires, J. (2022). The Politics of Cybersecurity in the Middle East. Oxford University Press.

Kumar, J., Santhanavijayan, A., Janet, B., Rajendran, B., & Bindhumadhava, B. S. (2020). Phishing Website Classification and Detection Using Machine Learning. En 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). doi: 10.1109/ICCCI48352.2020.9104161

Rajagopal, & Ramesh, B. (2016). Business Analytics and Cyber Security Management in Organizations. IGI Global.

ISSN: 2773-7527
Volumen 6. No. 1
Mayo 2024

Stair, R., & Reynolds, G. (2020). Principles of Information Systems. Cengage Learning.

Hole, K. J. (2015). Toward Anti-fragility: A Malware-Halting Technique. IEEE Security & Privacy, 13(4), 40-46. https://doi.org/10.1109/MSP.2015.73

Steele, C. (2020). What is Mobile Application Management (MAM)? Recuperado el 6 de mayo de 2022, de https://www.techtarget.com/searchmobilecomputing/definition/mobile-application-management-MAM

Sombatruang, N., Kadobayashi, Y., Sasse, M. A., Baddeley, M., & Miyamoto, D. (2018). The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan. En 2018 16th Annual Conference on Privacy, Security and Trust (PST) (pp. 1-11). doi: 10.1109/PST.2018.8514208

Sobh, T. (2013). Wi-Fi Networks Security and Accessing Control. International Journal of Computer Network and Information Security, 5(7), 9-20. https://doi.org/10.5815/ijcnis.2013.07.02

IBM. (2020). What is end-to-end encryption? Recuperado el 6 de mayo de 2022, de https://webcache.googleusercontent.com/search?q=cache:MZoi2awKfiIJ:https://www.ibm.com/topics/end-to-end-encryption+&cd=20&hl=es&ct=clnk&gl=ec

Vandenberg, D. T. (2017). Encryption Served Three Ways: Disruptiveness as the Key to Exceptional Access. Berkeley Technology Law Journal, 32, 531-562.

Yadav, A., & Prasad, L. B. (2019). IOT Devices for Control Applications: A Review. En 2019 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 473-479). doi: 10.1109/ICECA.2019.8821895

Infoblox. (2021). Infoblox Reporting and Analytics | Know Your Network. Recuperado el 6 de mayo de 2022, de https://www.infoblox.com/products/reporting-analytics/

Infoblox. (2021). IoT Security | Foundational Security for Botnet Protection. Recuperado el 6 de mayo de 2022, de https://www.infoblox.com/solutions/secure-iot/

Salih, H. M., & Mohammed, M. S. (2020). Spyware Injection in Android using Fake Application. En 2020 International Conference on Computer Science and Software Engineering (CSASE) (pp. 100-105). doi: 10.1109/CSASE48920.2020.9142101

IBM. (2021). ¿Qué es la seguridad móvil? Recuperado el 5 de mayo de 2022, de https://www.ibm.com/topics/mobile-security

IBM. (2021). Soluciones de gestión de movilidad empresarial (EMM). Recuperado el 6 de mayo de 2022, de https://www.ibm.com/security/enterprise-mobility-management

Camacho Hernández, O. (2015). Implementación de la gestión de la movilidad empresarial (enterprise mobility management - emm) para la gestion del correo corporativo en el departamento para la prosperidad social – DPS. Universidad Nacional Abierta y a Distancia. Recuperado el 18 de agosto de 2022, de http://repository.unad.edu.co/handle/10596/4852

Li, T., Mehta, A., & Yang, P. (2017). Security Analysis of Email Systems. En 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 91-96). doi: 10.1109/CSCloud.2017.20

Chandel, S., Yu, S., Yitian, T., Zhili, Z., & Yusheng, H. (2019). Endpoint Protection: Measuring the Effectiveness of Remediation Technologies and Methodologies for Insider Threat. En 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 81-89). doi: 10.1109/CyberC.2019.00023

Cando Estrella, C. A. (2020). Análisis e implementación de plataforma de seguridad para la protección de la información a través de la administración de los dispositivos finales en la Unidad Educativa Fiscomisional San Juan Bosco. Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones. Recuperado el 18 de agosto de 2022, de http://repositorio.ug.edu.ec/handle/redug/48833

Alshalan, A., Pisharody, S., & Huang, D. (2016). A Survey of Mobile VPN Technologies. IEEE Communications Surveys & Tutorials, 18(2), 1177-1196. https://doi.org/10.1109/COMST.2015.2496624

León Gómez, A. N. (2018). Monitoreo de rendimiento para la seguridad de VPN a través de PfSense y OpenVPN. Universidad Veracruzana. Facultad de Contaduría y Administración. Región Xalapa. Recuperado el 18 de agosto de 2022, de https://cdigital.uv.mx/

Gupta, A. K., Kumar, R., & Gupta, N. K. (2014). A trust based secure gateway selection and authentication scheme in MANET. En 2014 International Conference on Contemporary

ISSN: 2773-7527
Volumen 6. No. 1
Mayo 2024

Computing and Informatics (IC3I) (pp. 1087-1093). doi: 10.1109/IC3I.2014.7019816

Bienhaus, D., Ebner, A., Jäger, L., Rieke, R., & Krauß, C. (2021). Secure gate: Secure gateways and wireless sensors as enablers for sustainability in production plants. Simulation Modelling Practice and Theory, 109, 102282. https://doi.org/10.1016/j.simpat.2021.102282

Yahya, Z. B., Ktata, F. B., & Ghedira, K. (2016). Multi-organizational Access Control Model Based on Mobile Agents for Cloud Computing. En 2016 IEEE/WIC/ACM International Conference on Web Intelligence (WI) (pp. 656-659). https://doi.org/10.1109/WI.2016.0116

Agrawal, N., & Tapaswi, S. (2019). A trustworthy agent-based encrypted access control method for mobile cloud computing environment. Pervasive and Mobile Computing, 52, 13-28. https://doi.org/10.1016/j.pmcj.2018.11.003

Leal, E. (2019, febrero). La seguridad de la información en dispositivos móviles personales de uso profesional. Recuperado el 18 de agosto de 2022, de http://repository.unipiloto.edu.co/handle/20.500.12277/4920

Balbix Inc. (2020, mayo 7). Balbix Releases State of Password Use Report 2020. Recuperado el 6 de mayo de 2022, de https://www.businesswire.com/news/home/20200507005204/en/Balbix-Releases-State-of-Password-Use-Report-2020

Prensario, T. (2021, julio). Informe de Seguridad Móvil 2021 de Check Point. Recuperado el 6 de mayo de 2022, de https://prensariotila.com/33106-informe-de-seguridad-movil-2021-de-check-point/

Ulloa Hallo, A. G. (2021, diciembre). Análisis de problemas técnicos y legales de ciberseguridad y sus posibles soluciones en el contexto de la computación en la nube. Recuperado el 18 de agosto de 2022, de http://repositorio.puce.edu.ec:80/xmlui/handle/22000/19745

Schmitt, M. (2022, julio 17). Mobile Security for the modern CEO: Attacks, Mitigations, and Future Trends. arXiv. https://doi.org/10.48550/arXiv.2207.08105

VMware. (2022). What is Mobile Device Security? Recuperado el 5 de mayo de 2022, de https://www.vmware.com/topics/glossary/content/mobile-device-security.html