Fd-Rie
Formación docente
revista iberoamericana de educación

Artículo

Metodologia para gerenciar a segurança do computador para a Internet das Coisas

Methodology for managing computer security for the Internet of Things
Metodología de gestión de seguridades informáticas para internet de las cosas

Ivette Mateo Washbrum
Master en Ingeniería de Software y Sistemas Informáticos, Docente de la carrera de Redes, ITSVR
imateo33@gmail.com, Guayaquil - Ecuador, https://orcid.org/0000-0002-7523-7219

Recibido 19 Março de 2019 - Aceito em 9 de abril de 2020
Formación docente - revista iberoamericana de educación

http://www.revista-iberoamericana.org/index.php/es/index

e-ISSN: 2737-632X

Vol - 3 No. 2, abril - junho de 2020
Pags 40 - 50

Resumo. A rede de coisas, objetos e dispositivos conectados à Internet está crescendo exponencialmente, uma vez que a implantação e o design de equipamentos foram realizados de uma maneira muito diversificada, uma vez que não há Internet das coisas IoT padrão, razão pela qual o controle e o gerenciamento da segurança do computador nas redes de conexão de dispositivos com a Internet das Coisas se tornaram pesados. O desenvolvimento de um protocolo padrão para a Internet das Coisas foi considerado, considerando as especificações dos dispositivos existentes e as tecnologias de comunicação atuais, como aquelas em fase de implantação baseadas no 5G. Com base no protocolo padrão da Internet das Coisas, é proposta uma metodologia de gerenciamento de riscos e segurança de computadores para dispositivos IoT.

Palavras-chave: Metodologia, Segurança, Conexão, Dispositivos IoT.

Resumen La red de internet de las cosas, objetos y dispositivos conectados al internet está creciendo exponencialmente, debido a que el despliegue y diseño de equipos se ha realizado de forma muy diversificada, ya que no se dispone de un estándar de internet de las cosas IoT, por lo que se ha hecho engorroso el control y gestión de seguridades informáticas en las redes de conexión de dispositivos al internet de las cosas. Se ha planteado el desarrollo de un protocolo estándar para internet de las cosas, considerando las especificaciones de los dispositivos existentes y las tecnologías de comunicación vigentes, como las que se encuentran en etapa de despliegue basadas en 5G. Basado en el protocolo estándar de internet de las cosas, se propone una metodología de gestión de riesgos y seguridades informáticas para dispositivos IoT.

Palabras clave: Coaching, Coaching educativo, educación, pedagogía, educación superior, competencias.

Abstract. The internet of things, objects and devices network connected to the internet is growing exponentially, since the deployment and design of equipment has been carried out in a very diversified way, since there is no IoT internet of things standard, reason why the control and management of computer security in the connection networks of devices to the internet of things has become cumbersome. The development of a standard protocol for the Internet of Things has been considered, considering the specifications of existing devices and current communication technologies, such as those in the deployment stage based on 5G. Based on the standard internet of things protocol, a methodology of risk management and computer security for IoT devices is proposed.

Key words: Methodology, Security, Connection, IoT Devices.

INTRODUÇÃO

As propriedades autônomas de alguns objetos, como: smartphones, tablets, relógios, pulseiras, equipamentos de controle de telemedicina, televisões, equipamentos de controle de automação residencial, carros, etc; eles precisam estar sempre conectados à rede da Internet para atualizações ou envio de informações, como conseqüência dos padrões de vida atuais dos usuários, que por conveniência realizam suas atividades diárias com a ajuda e a dependência desses dispositivos, agravando a insegurança desde Ignorância: eles não tomam cuidado com as informações que seus equipamentos inteligentes enviam pela rede da Internet e, portanto, não tomam as precauções para modificar as configurações de segurança padrão que esses objetos de IoT possuem.

Dado o crescimento das conexões de dispositivos inteligentes à Internet, a evolução da IoT e a disseminação dos serviços de nuvem pública, existem mais vulnerabilidades e riscos no tráfego de informações transmitidas pela Internet, que podem ser interceptadas por terceiros. e corrompa os dados originais. (IBM.COM, 2017)

Para os fabricantes, o inconveniente surge porque os objetos da IoT são projetados para uma finalidade específica e, portanto, nem todos os aspectos que envolvem as salvaguardas gerais dos equipamentos da IoT são considerados e uma metodologia padrão para o desenvolvimento de aplicativos não foi considerada. IoT, cujas validações de segurança foram satisfatórias para qualquer plataforma. (MICROSOFT.COM, 2017)

É proposto de maneira padronizada o desenvolvimento da metodologia de segurança do computador que gerencia os riscos das conexões dos dispositivos IoT.

Verificando as políticas de segurança aplicadas às conexões de dispositivos IoT, propondo um sistema geral de conexões de dispositivos inteligentes que

combina os cenários dos modelos de comunicação IoT atuais. Estabelecer os processos de verificação da revisão de vulnerabilidade nos programas e aplicativos de equipamentos inteligentes, desde o desenvolvimento e codificação de software seguro, com a geração de um certificado e assinatura de segurança antes de seu lançamento e produção na IoT.

MATERIAIS E MÉTODOS

ma metodologia generalizada, que combina boas práticas para gerenciar riscos em um sistema para conectar objetos inteligentes à Internet das Coisas, revisando os principais fatores de segurança do sistema de conexão IoT.

1.- Definir processos de verificação de vulnerabilidades para mitigar riscos no hardware e software de dispositivos inteligentes.

2.- Propor um guia para revisar falhas de segurança nas comunicações estabelecidas em cada conexão de dispositivos IoT através da Internet com usuários ou plataformas em nuvem. (ENISA, 2017)

3.- Estabelecer processos de verificação de vulnerabilidades nas aplicações Plataformas e Nuvem.

São identificados os requisitos, a descrição, para o desenvolvimento, aplicação e avaliação da metodologia de gerenciamento de segurança de computadores do sistema de dispositivos inteligentes conectados à Internet das coisas.

A identificação de requisitos de desenvolvimento para a metodologia de gerenciamento da segurança de computadores do sistema de conexão de dispositivos da Internet das Coisas requer a colaboração de provedores de serviços em nuvem e fabricantes de dispositivos inteligentes.

RESULTADOS

A partir da pesquisa realizada, foi demonstrado que não existem protocolos genéricos de IoT, o que complica o estabelecimento de uma metodologia generalizada de gerenciamento de segurança na IoT.

É necessário ter como base as especificações dos protocolos genéricos de IoT, para o design de dispositivos inteligentes, que devem incluir considerações de segurança, uma vez que essas equipes compõem as redes IoT da Internet das Coisas e a metodologia proposta seria amplamente aplicado às redes de conexão IoT.

As especificações do protocolo IoT geral são estabelecidas:

☐ Compatibilidade com protocolos existentes: IP, TCP, UDP, TLS, DTLS, 802.11, 805.15, ZigBee, Zwave, CoAP, LTE, WirelessHart; LoRaWAN, MQTT, Json, Oauth; etc.

☐ Arquitetura de segurança de canais seguros, para garantir a integridade do sistema.

☐ A rede ad hoc que pode ser acessada por qualquer dispositivo externo e ambiente de trabalho.

☐ Firewall entre as entidades da camada de aplicação.

☐ Políticas de acesso, no modelo de confiança aberta, para permitir credenciais compartilhadas reduzindo o custo.

Credenciais de 128 bits.

☐ Os serviços fornecidos por este protocolo devem usar variações da chave de link em uma direção para evitar riscos de segurança.

☐ A distribuição das chaves por camadas é garantir a segurança da rede.

☐ Será designado um dispositivo que atuará como um centro de confiança que distribuirá as chaves.

☐ O dispositivo central confiável terá uma chave de inicialização padrão e o endereço IP da matriz.

☐ Os dispositivos aceitarão apenas conexões geradas com uma chave transmitida pelo centro de confiança, com exceção da chave inicial primária.
☐ Como exceção, o acesso às credenciais da rede será fornecido aos dispositivos que se registram pela primeira vez na rede.
☐ O emparelhamento para registro do equipamento e objetos inteligentes será feito por meio de códigos ou um PIN exclusivo para cada dispositivo, esses valores mobiliários permitem conformidade com os padrões de criptografia para transmissões entre nós.
☐ A segurança dos dados é de responsabilidade da camada que envia o quadro.
☐ Os quadros de dados serão criptografados, para impedir o tráfego não autorizado de equipamentos maliciosos do usuário. (ISO.ORG, 2017)
Com base no acima, a arquitetura de rede da Internet das Coisas é especificada.
☐ Interfaces compatíveis com o protocolo IoT entre redes de sensores e outras redes para aplicativos de sistema de rede inteligente.
☐ Arquitetura de rede de sensores baseada em protocolo IoT para suportar sistemas inteligentes.
Interface IoT entre redes de sensores com sistemas de rede inteligentes.
☐ Aplicativos e serviços emergentes baseados em redes de sensores de IoT para suportar sistemas de redes inteligentes. (CASTELLANOS, 2017)

CONCLUSÕES

La conexión de equipos inteligentes hacia Internet genera nuevos escenarios de casos de uso. Algunos utilizan Internet Protocol Suite que les ofrece mayor capacidad de procesar y obtener información de datos que recoge la red de sensores, que poseen estos dispositivos, la combinación de información que se puede obtener de estos equipos y sus redes sensoriales y neuronales,

ocasionan más vulnerabilidades y riesgos a los que se exponen los dispositivos y usuarios del IoT. (TEJERO, 2017)

El desarrollo de sistemas de redes IoT, que involucran redes de sensores, neuronales, la interacción con equipos y protocolos de comunicación inalámbricos, conlleva a los diseñadores de hardware y software para IoT a considerar los siguientes aspectos:

- Tiempo de operación del dispositivo, consideraciones de energización.
- Interacción a través de sensores u otro tipo de red.
- Tipos de conexión soportados hacia la red.
- Tipos de mantenimiento y actualización del dispositivo.
- Modelo de seguridad aplicable al dispositivo. (TINAJERO, 2017)

Por lo que se requiere información de tecnologías y protocolos de IoT utilizadas para el diseño de objetos y sistemas de interconexión de internet de las cosas.

Es justamente en la etapa de diseño de hardware y software que se debe tomar las consideraciones necesarias para evitar que las vulnerabilidades de seguridad de los equipos y aplicaciones sean aprovechadas por terceros inescrupulosos quienes pueden corromper la información. (INTERNET A.B., 2017)

Los protocolos de IoT deben ser aplicados a los entornos en los que se conectan los dispositivos, y considerarse en el diseño de hardware y software, la posibilidad de reconfiguración adaptándose a la necesidad y requerimiento del usuario. (ELIZALDE, 2016)

La infraestructura de la red de Internet, los dispositivos, y aplicaciones IoT evolucionan en el transcurso del tiempo, por lo que las consideraciones de diseño y seguridad en Hardware y software deben evolucionar conjuntamente.

De la investigación se concluye que en la actualidad no se dispone de una plataforma IoT que provea todas las facilidades requeridas para verificación y pruebas propuestas en la metodología de gestión de seguridades IoT.

Se recomienda trabajar en la estandarización de equipamiento hardware y software para internet de las cosas.

Se requiere el desarrollo de plataformas integrales de internet de las cosas que suministren herramientas para revisión automática de mecanismos de los dispositivos, así como la verificación por defecto de la codificación del software de las aplicaciones de dispositivos inteligentes y de aplicaciones en la nube.

Las plataformas actuales fueron desarrolladas prioritariamente para trabajar con sistemas diseñados para trabajar en sus plataformas tal es el caso de AWS y Azure, por lo que la adaptabilidad de dispositivos que operen con protocolos propietarios de otros proveedores, requiere el desarrollo de interfaces que les permitan integrar estos equipos a las plataformas existentes.

La estandarización demanda que se establezcan políticas de seguridad para compartición de servicios e infraestructura de los proveedores de Cloud, actualmente no se dispone de este tipo de políticas según lo indicado por la Alianza de Seguridad en la Nube CSA y el Concejo de Ciber Defensa CDC.

REFERÊNCIAS

ALLIANCE CYBER SECURITY. (DICIEMBRE de 2016). *https://downloads.cloudsecurityalliance.org/*. Obtenido de https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

Barros-Bastidas, C., & Turpo, O. (2020). La formación en investigación y su incidencia en la producción científica del profesorado de educa- ción de

una universidad pública de Ecuador. Publicaciones, 50(2), 167–185. doi:10.30827/publicaciones.v50i2.13952

Barros, C., & Turpo, O. (2017). La formación en el desarrollo del docente investigador: una revisión sistemática. Revista Espacios, 38(45).

CASTELLANOS, J. (OCTUBRE de 2017). *https://www.exploit-db.com/*. Obtenido de https://www.exploit-db.com/docs/spanish/43160-reversing-and-exploiting-iot-devices.pdf

Castañeda, JG., Camargo, JA y Londoño, MK. (2018). Análisis bibliométrico como herramienta para el seguimiento de instrumentos psicológicos validados en Colombia. Revista Ibérica de Sistemas e Tecnologias de Informação, E18, 38-46.

Daza, J., Castañeda, JG., Tovar, C., Segovia, C y Cortés, JE. (2019). Diseño y análisis psicométrico de una prueba para medir la percepción de clases frente a la formación integral de estudiantes universitarios «PCFI». Espacios, 40 (2), 18-29.

ELIZALDE, D. (DICIEMBRE de 2016). *https://techproductmanagement.com/*. Obtenido de https://techproductmanagement.com/iot-decision-framework/

ENISA. (20 de NOVIEMBRE de 2017). *https://www.enisa.europa.eu*. Obtenido de https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

IBM.COM. (MAYO de 2017). *https://www.ibm.com/*. Obtenido de https://www.ibm.com/developerworks/library/iot-trs-secure-iot-solutions1/index.html

INTERNET A.B. (OCTUBRE de 2017). *https://tools.ietf.org/*. Obtenido de https://tools.ietf.org/html/rfc6347

ISO.ORG. (NOVIEMBRE de 2017). *https://www.iso.org*. Obtenido de https://www.iso.org/standard/

MICROSOFT.COM. (DICIEMBRE de 2017). *https://azure.microsoft.com/*. Obtenido de https://azure.microsoft.com/en-us/updates/microsoft-azure-iot-reference-architecture-available/

OWASP.ORG. (ENERO de 2018). *https://www.owasp.org*. Obtenido de https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

PALMES. (2010). *PDCA: PLANIFICAR, HACER, VERIFICAR, ACTUAR. MADRID: AENOR. ASOCIACION ESPAÑOLA DE NORMALIZACION Y CERTIFICACION*. MADRID.

TEJERO, A. (FEBRERO de 2017). *https://www.researchgate.net/*. Obtenido de https://www.researchgate.net/publication/313400021_Metodologia_de_analisis_de_riesgos_para_la_mejora_de_la_seguridad_del_Internet_de_las_Cosas_Caso_Smartwatch?enrichId=rgreq-3bbb99f0acf96b6624d901d73697e9c2-XXX&enrichSource=Y292ZXJQYWdlOzMxMzQwMDAyMTtBUzo

TINAJERO, A. (FEBRERO de 2017). *https://www.researchgate.net*. Obtenido de https://www.researchgate.net/profile/Alberto_Tejero/publication/313400021_Metodologia_de_analisis_de_riesgos_para_la_mejora_de_la_seguridad_del_Internet_de_las_Cosas_Caso_Smartwatch/links/58

9976e34585158bf6f795db/Metodologia-de-analisis-de-riesgos-para-la

VIOLINO, C. (ENERO de 2018). *https://www.csoonline.com/*. Obtenido de https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html

von Feigenblatt, Otto Federico, A Socio-Cultural Analysis of Romantic Love in Japanese Harem Animation: A Buddhist Monk, a Japanese Knight, and a Samurai (September 16, 2010). Journal of Asia Pacific Studies, Vol. 1, No. 3, pp. 636-646, 2010, Available at SSRN: https://ssrn.com/abstract=1760643

von Feigenblatt, Otto Federico, Costa Rica's Foreign Policy: Can 'Right' Become 'Might'? (November 27, 2008). Journal of Alternative Perspectives in the Social Sciences, Vol. 1, No. 1, pp. 11-15, 2008, Available at SSRN: https://ssrn.com/abstract=1308245

von Feigenblatt, Otto Federico, Human Security and the Responsibility to Protect: A Holistic Approach to Dealing with Violent Conflict in Southeast Asia (May 13, 2009). Journal of Social Sciences, Vol. 11, No. 1, pp. 27-40, 2009, Available at SSRN: https://ssrn.com/abstract=1570171