Auditoria de seguretat d'una aplicació mòbil amb accés a un entorn SAP

Unitat: Seguretat TIC
AREA: Ciberseguretat TMB
Data: 17 de maig 2024

Juan Jose del Rio Estevez
Responsable Monitorització i
Adm. de Sistemes

Transports
Metropolitans
de Barcelona

Índex

1. Realització d'auditoria de seguretat d'una aplicació de dispositiu mòbil amb accés a entorn SAP

1.1 Introducció

L'Àrea de Tecnologia de TMB té la responsabilitat de definir, implantar i controlar la seguretat lògica en tots els entorns TIC i la física quant a les dependències dels CPD on es troben els equips TIC.

Dins d'aquesta responsabilitat s'inclou la de realitzar auditories en els sistemes dels quals és responsable per comprovar el seu nivell de seguretat i proposar les millores necessàries per a la seva millora.

També es troba dins de la seva responsabilitat comprovar que les aplicacions que es posen a disposició dels seus empleats estan dotades d' un nivell de seguretat acceptable.

1.2 Objecte

L'objecte d'aquest document és la sol·licitud de la realització d'una auditoria de seguretat sobre una aplicació mòbil que accedeix a un entorn SAP.
Se n'han d'oferir divuit (18) auditories i s'ha de tractar com si fos una nova auditoria cadascuna d'elles. Es preveu fer les auditories a un ritme, com a màxim, de una auditoria per S. O. (Android i iOS) per quadrimestre, es a dir sis (6) a l'any.
El període de temps de les auditories s'estima fins a cinc (5) anys.

2. Objecte de sol·licitud

2.1 Auditoria mòbil d'accés a un entorn SAP.

Es procedirà a auditar en mode caixa blanca l'aplicació desenvolupada per TMB per a l'accés a les dades emmagatzemades en els sistemes de SAP HR o d'altres entorns de TMB

- Anàlisi de l'aplicació mòbil per a la detecció de vulnerabilitats.
- L'anàlisi pot realitzar-se tant per a sistemes Android com iOS.
- Valoració dels riscos a partir de les vulnerabilitats detectades.

A més, s'ha de realitzar una auditoria de seguretat en mode caixa blanca o gris de l'entorn SAP al qual accedeix l'aplicació amb l'objectiu de:

- Analitzar la seguretat dels servidors que componen l'entorn per a la detecció de vulnerabilitats.
- Anàlisi de seguretat dels serveis que intervenen en l'entorn per detectar vulnerabilitats.
- Dur a terme una anàlisi de la infraestructura per proposar millores en cas necessari.

2.2 Lliurables

Un cop finalitzades les auditories s'ha de fer lliurament d'un document on es reculli, al menys, el següent:

- Data de l'auditoria.
- Versió dels productes i aplicacions auditades.
- Proves executades en sistemes i aplicació.
- Resum executiu.
- Llistat de vulnerabilitats detectades i regs associats.
- Accions proposades per mitigar els riscos i per a cadascuna d'elles:
    - Cost de resolució
    - Riscos mitigats
- Pla d'acció proposat.

2.3 Altres consideracions

Com s'ha indicat en el punt 1.2 aquestes auditories s'hauran de realitzar en divuit (18) ocasions, totes elles com si fossin una nova auditoria. L'inici de cadascuna d'elles vindrà determinat per la sol·licitud de l'equip de TMB que necessita l'auditoria d'una aplicació.

També s'ha d'incloure un suport post auditoria que verifiqui que les mesures i controls implementats compleixin el seu objectiu (recheck de l'aplicació i sistemes auditats), realitzant la documentació de tot això.

3. Característiques generals

3.1 Confidencialitat

L'empresa col·laboradora ha d'acceptar el compromís de confidencialitat respecte a les dades a les quals tindrà accés i que són propietat de TMB. De la mateixa manera s'ha de comprometre a seguir la Política de Ciberseguretat de TMB i la Normativa d'ús de mitjans electrònics de TMB.

Els permisos d'accés als sistemes i aplicació, en cas de ser necessari, tindran el nivell necessari per al treball a realitzar i assignats a usuaris personals.

En cas de precisar de l'accés amb un usuari amb privilegis elevats en el sistema es durà a terme a través de l'eina que disposa TMB per a aquest fi, de manera que quedin traçades les accions que es realitzin.

3.2 Aspectes funcionals

La prestació del servei objecte d'aquesta contractació ha de complir amb els ítems següents:

a. La realització de les tasques presencials, de no indicar una altra cosa, es realitzaran a l'oficina situada a l'adreça següent:

   Centre de Suport Tecnològic
   C/Josep Estivill, 47
   08027, Barcelona

   Es pot valorar l'elaboració de treballs en remot sempre que s'acordi l'abast dels mateixos.

b. El projecte, en la part del contractista, disposarà d'un referent que serà l'interlocutor amb el responsable del projecte de TMB i es disposaran dels recursos necessaris per finalitzar les tasques en les dates acordades.

c. Es presentarà una planificació dels treballs a realitzar per acordar amb TMB la durada del treball en cas que es tracti de tasques que permetin aquesta planificació.

d. L'horari de les jornades serà de 8h a 15h de dilluns a divendres.

3.3 Contacte

El contacte amb TMB per resoldre qualsevol dubte és:

- Nom: Juan José Del Río Estévez
- Correu: jjdelrio@tmb.cat
- Telèfon: 932 987 450