UNIVERSITAT DE BARCELONA

Àrea de Tecnologies de la Informació i la Comunicació
Pavelló Rosa
Travessera de les Corts, 131-159
08028 Barcelona
Tel. +34 934 021 737
Fax +34 934 021 505

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DELS SERVEIS D'ELABORACIÓ D'UN INFORME DE CIBERSEGURETAT I SERVEIS GESTIONATS DE LA PLATAFORMA MICROSOFT OFFICE365 PER A L'ÀREA DE TECNOLOGIES DE LA INFORMACIÓ I LA COMUNICACIÓ DE LA UNIVERSITAT DE BARCELONA (ATIC)

EXPEDIENT 2025-189

1. OBJECTIU

La Universitat de Barcelona (UB) té la necessitat de fer el seguiment de la millora contínua de la ciberseguretat.

- Informe de ciberseguretat

L'informe de seguiment de la ciberseguretat es presentarà mensualment i es basarà en les dades (logs) recollits de diferents plataformes que caldrà configurar per lliurar-les al SIEM Sentinel de Microsoft ja en producció i aplicar-ne casos d'ús.

- Servei Gestionat SIEM Sentinel de Microsoft: Anàlisi, creació de casos d´ús a i automatització.
- Serveis Gestionats Office365

Els Serveis Gestionats de Microsoft Office365 es basaran en reunions periòdiques de seguiment amb els diferents responsables ATIC per tal de millorar la ciberseguretat proposant millores a les diferents configuracions i proves de concepte de les aplicacions incloses a la plataforma Microsoft Office 365. S'inclou com a Servei Gestionat la plataforma Microsoft Sentinel (SIEM).

2. INFORME DE CIBERSEGURETAT I SERVEI GESTIONAT SIEM MICROSOFT SENTINEL

2.1 Necessitats

2.1.1 Un Informe de Ciberseguretat

L'informe de seguiment de la ciberseguretat es presentarà mensualment a tècnics i Direcció ATIC.

Es mantindrà l'informe amb les dades recollides del SIEM Microsoft Sentinel a la plataforma d'informes del mateix Microsoft Sentinel o a la plataforma PowerBI ja contractada mostrant una consola amb els diferents indicadors de seguretat.

Es presentarà mensualment l'informe utilitzant un suport en Power Point on s'expliquin els diferents indicadors i els valors enllaçats a la plataforma d'informes per consultar tendències en qualsevol moment de la presentació. S'esperen millores en la presentació enllaçant amb les dades de SIEM o del PowerBI.

L'informe proposarà millores a realitzar en matèria de ciberseguretat que hauran de ser implantades en el seguiment dels Serveis Gestionats Microsoft Office 365.

L'informe mostrarà el riscos més importants associats a les diferents fons de dades de ciberseguretat i com reduir-los.

L'informe farà un seguiment de les millores proposades.

L'informe es basa en uns indicadors de ciberseguretat (KPSI) que es calculen en base a les dades extretes de les diferents eines de ciberseguretat. Dins de l'informe caldrà mostrar els indicadors KPSI en funció del Catàleg de Serveis de la UB anomenats essencials per l'ENS.

Els indicadors es calculen a la plataforma d'informes en base a les fonts de dades recollides al SIEM.

Les fonts de dades del SIEM poden ser:

- Logs d'eines de seguretat de la UB en diferents formats transportats via RSYSLOG o similar.
- Logs d'eines de seguretat al núvol de diferents proveïdors. Normalment s'obtenen via API.
- Importació de fitxers CSV periòdic si no es pot fer d'altra manera.

Es proporcionarà una llista d'indicadors de seguretat actuals als licitadors.

Es proporcionarà l'arquitectura actual de seguretat als licitadors.

Existeix un informe de seguretat basat en PowerBI, per millorar, que es compartirà amb els licitadors.

2.1.2 Un Servei Gestionat de la plataforma SIEM Microsoft Sentinel.

Instal·lació i configuració del maquinari necessari per tal de recollir la informació de les diferents fonts de dades (logs o API). Actualment ja existeix un servidor a Azure de recol·lecció de syslog.

Configuració del maquinari originari de les dades. Típicament syslog.

Desenvolupament del programari necessari per recollir dades. Típicament via API.

L'adjudicatari proposarà nous indicadors de seguretat o modificarà els existents en base a les millores proposades i les noves fonts de dades per incorporar a l'informe de ciberseguretat.

Anàlisi del SIEM per trobar comportaments maliciosos i correlacions entre les dades.

Implementació de Casos d'ús:

- Creació d'alarmes, tickets d'incident de seguretat a la plataforma JIRA UB i automatismes en base a l'anàlisi. Els automatismes poden ser dirigits a qualsevol element de control de la seguretat a la UB, típicament tallafocs o programari accessible via API.

- Calen guies, procediments i automatismes d'actuació dels següents punts:

  - Anàlisi de tendències per a la identificació i optimització de polítiques seguretat.
  - Recomanacions i guies sobre esdeveniments catalogats com a incidents de seguretat.
  - Informes sobre incidents de seguretat greus.
  - Monitoratge de la ciberseguretat en temps real dels esdeveniments importants de diverses plataformes o origen de dades (seguretat, sistemes, aplicacions, bases de dades, estacions de treball, etc.).

- Agents IA d'ajuda

3. SERVEIS GESTIONATS MICROSOFT OFFICE365

3.1 Necessitats

3.1.1 Reunions periòdiques de millora del indicadors de seguretat de Microsoft Office365

Els Serveis Gestionats de Microsoft Office365 es basaran en reunions periòdiques, mínim setmanals, de seguiment amb els diferents responsables ATIC per tal de millorar la ciberseguretat proposant millores a les diferents configuracions i proves de concepte de les aplicacions incloses a la plataforma Microsoft Office 365.

3.1.2 Valorar impacte i aplicar millores de seguretat de Microsoft Office365

Es busca augmentar el Security Score de Microsoft seguint les recomanacions de cada acció.

Valorar si aquestes accions tenen impacte econòmic segons el llicenciament actual.

Proposar polítiques més segures a la plataforma.

Fer proves d'impacte inicial de l'aplicació d'una política.

Manuel Pérez Castillo
Cap d'Infraestructures
Àrea TIC