AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

Informe del servei Catalonia SOC Consorci Administració Oberta de Catalunya

Període: del 25/08/2022 al 25/08/2022

Data: 26-08-2022

Índex

Què conté aquest informe del servei Catalonia SOC?

L'Agència de Ciberseguretat de Catalunya governa i disposa del servei públic de ciberseguretat per a les administracions locals composat d'un conjunt de prestacions:

1. Eines de coneixement i governança: A través del portal de seguretat per a les administracions locals proveeix recursos de coneixement, informes tècnics, marc normatiu, models documentals, continguts de formació i conscienciació, etc.
2. Plataforma Cloud Catalonia SOC per al desplegament de solucions de ciberseguretat per a administracions locals.
3. Capacitat de resposta als incidents de ciberseguretat al món local, a través del Catalonia-CERT.

Us presentem aquest Informe d'alertes de seguretat i informació de volumetries de navegació (garantint el compliment de la GDPR) amb el període sol·licitat per al teu ens per la informació proporcionada pels agents instal·lats en els dispositius d'usuaris o configurats per un túnel IPsec/GRE. La informació que es proporciona en aquest informe en format pdf permet prendre acció per diferents responsables de l'ens, però, seguint criteris de RGPD cal tenir en compte que, cal tenir en compte que s'evita expressament la compartició de dades personals dels usuaris implicats i que la informació pugui ser difosa fora del control de l'organització. Per trobar la informació de detall a què es refereix l'informe sobre els diferents usuaris cal fer-ne consulta puntual dins el portal web amb un perfil autoritzat.

Aquesta solució de ciberseguretat basada en seguretat cloud (SASE) permet l'aplicació de controls de seguretat basats en polítiques en el núvol per tal de garantir una navegació segura a Internet amb independència de la ubicació dels usuaris o dispositius.

En l'informe podreu trobar informació de detall i gràfics sobre:

- El possible robatori de credencials
- La fuita de dades
- L'explotació de vulnerabilitats
- La detecció de codi maliciós en diferents estats

A través del servei de Suport i informes de Catalunya SOC, que es posarà aviat en marxa, podreu gestionar incidències, peticions i consultes.

Glossari de termes que s'utilitzen en aquest informe

Usuari:
Cada usuari és identificat amb una bústia de correu o similar i serà reconegut per la solució SASE realitzant la instal·lació del Client. El programari Client s'instal·la en el dispositiu corresponent de cada usuari per poder capturar i analitzar el trànsit web amb l'objectiu de protegir l'organització.

Dispositiu:
Els dispositius detectats es classifiquen segons el sistema operatiu que tinguin instal·lat i sent els més populars: Windows i Mac OS X.

Navegador:
La solució SASE és capaç de capturar el trànsit des de diferents navegadors i a més captura el trànsit de les aplicacions natives instal·lades a l'ordinador de l'usuari (natives).

Categoria Web:
S'han predefinit una sèrie de categories per classificar les pàgines Web visitades. En total s'han utilitzat 110 categories Web i es mostra el nom de cadascuna d'elles al final d'aquest document.

Nivell de severitat dels malwares:
Index de severitat de l'alerta:

- **High**
- **Medium**
- **Low**

Índex de confiança (CCI/CCL):
La solució SASE adoptada fa servir un indicador de confiança per classificar el nivell de risc dels esdeveniments realitzats durant la navegació. Aquest indicador és un número del 0 al 100 (denominat com CCI) que s'assigna avaluant cada aplicació, segons més de 30 criteris objectius adaptats de la Cloud Security Alliance. En funció de la puntuació obtinguda, l'aplicació es col·loca en un dels 5 nivells de confiança al núvol que es mostren a continuació. CCL o Nivells de confiança al núvol:

- **Excellent**
- **High**
- **Medium**
- **Low**
- **Poor**

Podeu utilitzar aquesta puntuació per prendre decisions sobre l'ús d'aplicacions o per establir polítiques de seguretat per nivell de confiança. Aquest número es calcula segons les diferents capacitats de resposta de les aplicacions i utilitzant un algorisme d'aprenentatge automàtic. A més, la puntuació d'una aplicació pot ser recompensada o penalitzada segons la categoria a què pertanyi. Per exemple, per a una aplicació d'una xarxa social que no xifra les dades emmagatzemades no seria gaire alta. Tot i això, per a una aplicació d'emmagatzematge al núvol la penalització per no xifrar les dades seria molt més alta. Es mostren alguns exemples d'aplicacions amb diferents nivells de confiança segons la puntuació obtinguda de 0 a 100.

Resum executiu de l'informe

Gestió d'usuaris i de tiquets

Usuaris

Usuaris d'alta al servei	VPN vinculades al servei
5	0

Tiquets

Tiquets oberts	Tiquets resolts	Tiquets tancats
1	0	7

Indicadors de ciberseguretat

	Període actual 25/08/2022 - 25/08/2022	Període anterior 24/08/2022 - 24/08/2022
1. Alertes detectades	0	0
2. Credencials compromeses	0	0
3. Anomalies detectades en el comportament dels usuaris	0	0
4. Principals llocs bloquejats	42	37
5.1 Aplicacions amb nivell de confiança “Poor”	1	1
5.2 Aplicacions amb nivell de confiança “Low”	1	0

1. Alertes detectades

Es mostra el llistat d'esdeveniments que han detectat codi maliciós (malware) en llocs web o en axius que es trobin en trànsit, juntament amb el total d'esdeveniments i el número d'usuaris diferents que han generat aquell esdeveniment.
Es divideix en tres apartats segons el tipus d'activitat que l'usuari estava realitzant en el moment de l'event tant en búsqueda (navegador), pujades o descàrregues d'arxius*.

No s'han trobat dades

***Acció realitzada:** Detecció, alerta i bloqueig.

2. Credencials compromeses

Es mostren les dates on es detecta que l'usuari té les seves credencials exposades per possibles fuites d'informació.

No s'ha trobat dades

* **Recomanació:** actualitzar les contrasenyes periòdicament.

3. Anomalies detectades en el comportament dels usuaris

Es mostra el llistat d'alertes generades respecte al comportament dels usuaris.
En la taula s'indica el total d'esdeveniments i el nombre d'usuaris involucrats per aplicació.
Les alarmes generades poden ser les següents:

- *Moviment de dades sospitós*: Detecta la fuga de dades accidental o intencionada. Identifica el moviment de dades des d'instàncies d'aplicacions corporatives autoritzades a aplicacions/llocs personals o no corporatius.
- *Credencials compartides*: Detecta la compartició de credencials d'usuaris que puguin violar les polítiques de seguretat corporatives.
- *Pujades massives*: Detecta moviments de dades sospitosos → 100 fitxers/hora.
- *Eliminació massiva*: Supervisa els possibles usuaris de risc per detectar qualsevol activitat malintencionada que pogués provocar la pèrdua de dades → 100fitxers/hora.
- *Descàrregues massives*: Detecta descàrregues de dades sospitoses → 100 fitxers/hora.
- *Inicis de sessió erronis massius*: Identifica 3 intents fallits a l'interval de 15 minuts en algun compte dels usuaris.
- *Activitats estranyes*: Detecteu l'activitat de l'usuari que no sol ser habitual. Per exemple, l'usuari mai no ha baixat d'una aplicació en particular en els darrers 60 dies.
- *Països en risc*: Identifica l'accés/activitat dels usuaris que tenen lloc a països configurats com a països de risc.

No s'ha trobat dades

4. Polítiques de seguretat del trànsit d'Internet

Es mostren els esdeveniments bloquejats per les polítiques de seguretat de navegació.
En cadascuna de les taules es mostra el total d'esdeveniments, la pàgina web visitada referent i URLs bloquejades.

4.1 Política no definida

Aplicació	Web d'origen	URL	Total d'events	Total d'usuaris diferents
Dropbox	-	uc1905877722c301c9f8242ec8b6.previews.dr...	1	1
eicar	-	www.eicar.org/179e684b61aaf6652d85239a1c...	12	1

4.2 [Web] Blocar la navegació de pàgines web de països de risc

Aplicació	Web d'origen	URL	Total d'events	Total d'usuaris diferents
kaspersky-labs	https://www.kaspersky.es/	content.kaspersky-labs.com/se/es/content...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	api-router.kaspersky-labs.com/logger2/ex...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	api-router.kaspersky-labs.com/logger2/me...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	api-router.kaspersky-labs.com/offer/es/e...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1

Aplicació	Web d'origen	URL	Total d'events	Total d'usuaris diferents
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	2	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1

Aplicació	Web d'origen	URL	Total d'events	Total d'usuaris diferents
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/com/conten...	1	1
kaspersky-labs	https://www.kaspersky.es/small-to-medium...	content.kaspersky-labs.com/se/es/content...	1	1
kaspersky-labs	-	content.kaspersky-labs.com/9e0a3aef53123...	13	1
kaspersky-labs	-	content.kaspersky-labs.com/favicon.ico	16	1
kaspersky-labs	-	content.kaspersky-labs.com/se/com/conten...	6	1

Aplicació	Web d'origen	URL	Total d'events	Total d'usuaris diferents
kaspersky-labs	-	content.kaspersky-labs.com/se/com/conten...	9	1
kaspersky-labs	-	content.kaspersky-labs.com/se/com/conten...	1	1

5. Aplicacions de risc per ús

Es mostren les aplicacions utilitzades amb un menor nivell de confiança assignat per la solució SASE (nivell de confiança "Poor" o "Low") i el total d'events.
Per entendre bé el valor d'aquest CCI, podeu veure la informació a l'inici del document.

5.1 Aplicacions amb nivell confiança "Poor"

Nom de l'aplicació	Categoria	CCI	Total d'events
TikTok Inc	Social	16	1

5.2 Aplicacions amb nivell confiança "Low"

Nom de l'aplicació	Categoria	CCI	Total d'events
Youtube	Streaming & Downloadable Video	57	1

5.3 Aplicacions amb nivell confiança "Sota recerca"

Nom de l'aplicació	Categoria	CCI	Total d'events
Microsoft Office 365 Bypass	Technology	No definit	5
null	Business	No definit	3
null	Education	No definit	6
null	Government & Legal	No definit	11
null	No Content	No definit	1

Nom de l'aplicació	Categoria	CCI	Total d'events
null	Personal Sites & Blogs	No definit	9
null	Search Engines	No definit	6
null	Security	No definit	14
null	Technology	No definit	13
null	Travel	No definit	1

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

https://portalaall.ciberseguretat.cat