Seguretat, dades i integració

El 19 de juliol de 2024, milers de passatgers de l'aeroport de Palma van fer cua durant hores als taulells de facturació. No hi havia hagut cap atac. Una actualització defectuosa de CrowdStrike Falcon, un programa de seguretat, havia fet caure uns **8,5 milions d'ordinadors Windows** a tot el món, segons Microsoft. Aena va passar a procediments manuals. Va caure una peça de la qual depenia tot, i tot el que hi estava connectat es va aturar.

Cada tecnologia que vas afegir al pla la lliçó anterior porta dos regals: **dades noves**, que has de gestionar, i **portes noves**, que algú ha de tancar. I tot s'ha de connectar, així que també has de saber què passa quan una peça falla.

Què aprendràs

- Trobar les possibles **bretxes de seguretat** de cada àrea del teu pla, a partir de l'auditoria passiva del D5, i donar a cadascuna una mesura
- Definir com es **tracta** cada tipus nou de dades al llarg del seu cicle de vida
- Donar a cada objectiu estratègic un **indicador** amb una fórmula i una font de dades
- Dibuixar el **diagrama d'integració** de dades, aplicacions i plataformes a diagrams.net, amb la **font de referència** de cada dada
- Evitar el parany de les mesures genèriques ("instal·lar un antivirus") que no responen a cap bretxa concreta

Panys per a cada barri

En el joc de construir ciutats, la ciberseguretat és la policia, les murades i els panys. Un barri nou sense això és una invitació.

> Una **bretxa de seguretat**, en aquesta unitat, és un punt feble d'una àrea: una cosa que podria anar malament amb les seves dades o sistemes, per un atac, per un error o per accident.

No la confonguis amb una **violació de dades personals**: és un incident que ja ha passat, que el RGPD (Reglament (UE) 2016/679, article 33) diu que s'ha de notificar a l'autoritat "sense dilació indeguda i, si és possible, en un termini màxim de 72 hores" després que l'empresa en tengui coneixement. El teu pla analitza les bretxes perquè les violacions no arribin a passar.

Per a cada àrea: **quin actiu o quines dades hi ha, què podria anar malament, quina mesura hi poses i quina llei s'aplica.**

Àrea	Actiu o dades	Bretxa possible	Mesura	Llei
Comandes	Portal B2B amb comptes dels hotels	El personal de recepció de l'hotel comparteix una contrasenya	Un compte per persona, MFA, registre d'accessos	RGPD (dades de contacte)
Forns	Comptadors IoT a la xarxa de l'obrador	Dispositius amb contrasenyes de fàbrica a la mateixa xarxa que l'oficina	Xarxa separada per a l'OT, canviar les credencials	—

Àrea	Actiu o dades	Bretxa possible	Mesura	Llei
Qualitat	Registres de temperatura	Un sensor falla i ningú no s'adona que els registres s'han aturat	Alarma quan deixen d'arribar dades, còpia diària	Normativa de seguretat alimentària
Totes	Serveis al núvol de tercers	Dependència del proveïdor	Còpies de seguretat pròpies, contracte i ubicació de les dades comprovats	RGPD, NIS2 si s'aplica

El punt de partida per a la teva empresa és l'**auditoria passiva** del D5: les capçaleres de seguretat, les galetes i la política de privadesa del seu web públic.

> **Només passiva**
> Tot el que diguis de la seguretat de l'empresa real surt del que el seu web mostra a qualsevol visitant: securityheaders.com, Mozilla HTTP Observatory, les DevTools del navegador, el bàner de galetes, la política de privadesa. Mai no l'escanegis, mai no provis ports, mai no intentis iniciar sessió.

> **Compte: "instal·lar un antivirus"**
> Una mesura que no respon a una bretxa concreta és decoració. Si no pots dir quina bretxa tanca una mesura, esborra-la.

Entren dades, surten decisions

Cada tecnologia nova produeix dades noves: comandes del portal, consum dels forns, temperatures de les cambres. Per a cadascuna s'han de definir dues coses.

Tractament. El cicle de vida que vas fer servir al D5: com es recullen, on es guarden, qui hi pot accedir, quant de temps es conserven i com s'eliminen. Si són dades personals, s'apliquen el RGPD i la LOPDGDD (Llei orgànica 3/2018).

Anàlisi. Les dades t'han de dir si s'estan complint els objectius.

> Un **indicador** (o **KPI**, de l'anglès *key performance indicator*) és un nombre, calculat amb una fórmula fixa a partir de dades que tens, que mostra si s'està assolint un objectiu.

En el joc de construir ciutats, els indicadors són les capes de les vistes d'informació: trànsit, contaminació, felicitat. Cada objectiu de l'apartat 1 en necessita almenys un.

Objectiu	Indicador i fórmula	D'on surten les dades	Cada quant
Malbaratament	kg rebutjats o no venuts ÷ kg produïts	ERP (producció) i registre de devolucions	Setmanal
Comandes en línia	Comandes dels hotels pel portal ÷ totes les comandes dels hotels	Portal i ERP	Mensual
Energia	kWh dels forns ÷ kg produïts	Comptadors IoT i ERP	Mensual

Les canonades entre edificis

> La **integració** és com viatgen les dades entre aplicacions, i sobre quines plataformes funcionen aquestes aplicacions.

Pensa en tres capes:

Capa	Què conté	A l'obrador d'exemple
Dades	Clients, comandes, consums, temperatures	Cada dada té **una font de referència**: el client "viu" a l'ERP
Aplicacions	Els programes que fan servir les dades	Portal, ERP, quadre de comandament, model de previsió. Es comuniquen per mitjà d'**API**; les exportacions manuals són l'últim recurs
Plataformes	On funcionen les aplicacions	Serveis al núvol del D3, un dispositiu edge a l'obrador per als sensors

> La **font de referència** d'una dada és l'únic sistema on es crea i es corregeix; tots els altres sistemes la copien d'allà.

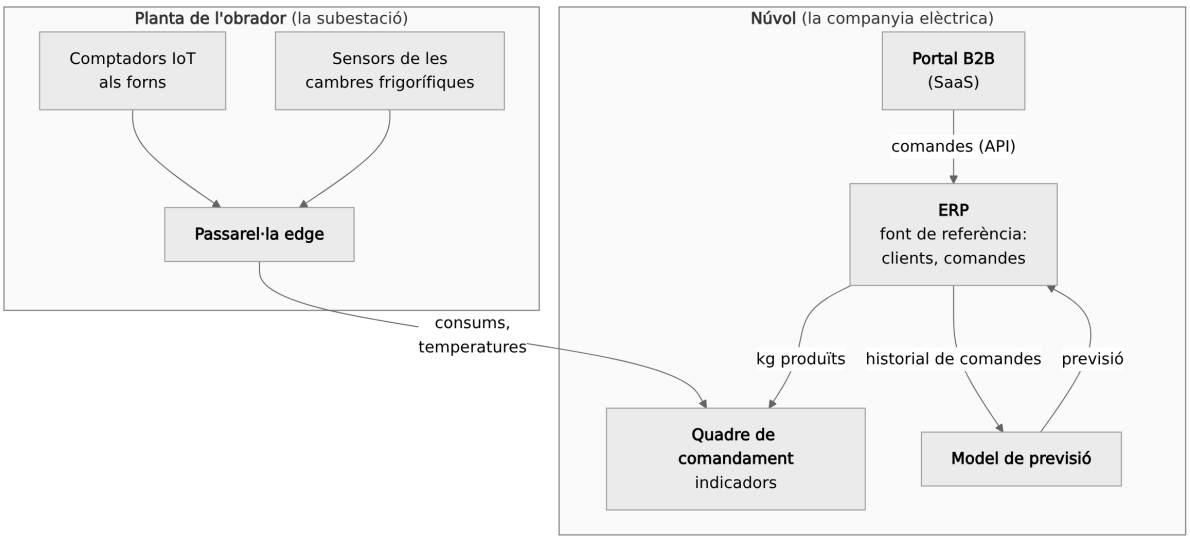
> Una **API** (interfície de programació d'aplicacions) és una porta que obre un programa perquè un altre programa li pugui demanar dades o enviar-n'hi, sense cap persona pel mig.

Aquest és el diagrama d'integració de l'obrador d'exemple, del mateix tipus que el que dibuixaràs:

Comprova cada diagrama amb tres preguntes: **on és la font de referència? com viatja la dada? què passa si cau una peça?** La història de l'aeroport de Palma és la resposta a la tercera pregunta quan ningú no se l'havia fet.

A classe: diagrama, bretxes i indicadors

Pas	Fes això	Hauries de veure
1 · grup	El Tècnic/a obre app.diagrams.net, tria **Device** (desar en aquest ordinador) i crea un diagrama en blanc. Els altres dicten a partir del D3 i de l'apartat 2	Un llenç buit



Pas	Fes això	Hauries de veure
2 · grup	Una caixa per aplicació, agrupades per plataforma (núvol, edge, local); fletxes etiquetades amb **què** hi viatja i **com** (API, fitxer, a mà); la font de referència de cada dada marcada	Un diagrama que algú de fora del grup podria llegir
3 · grup	**File › Export as › PNG**, i deseu també el fitxer `.drawio`	Dos fitxers: la imatge i el diagrama editable
4 · tot sol	Agafa **una àrea** del pla i escriu dues bretxes possibles, l'actiu afectat, una mesura per a cadascuna i la llei implicada. Almenys una ha de sortir de l'auditoria passiva del teu D5	Dues files a la taula compartida de bretxes
5 · tot sol	Escriu l'indicador d'**un** objectiu: nom, fórmula, d'on surten les dades al diagrama, cada quant	Un indicador que realment podries calcular

Lliura a Classroom (activitat de classe individual): les teves dues files de bretxes i el teu indicador, amb el diagrama del grup en PNG adjunt. Només passiva, i sense IA generativa.

Per al teu projecte

Aquesta lliçó construeix l'**apartat 3 · Seguretat i dades** del D6 · Pla de transformació (criteris g i h) i el diagrama d'integració de l'**apartat 4** (criteri i). Les bretxes parteixen de l'auditoria del teu D5; les plataformes surten de la teva arquitectura del D3. Si el D3 ja no encaixa amb les tecnologies de l'apartat 2, actualitza'l i escriu el canvi al registre de canvis.

Idees clau

- Una **bretxa de seguretat** és un punt feble d'una àrea; una **violació de dades personals** és un incident que ja ha passat, que s'ha de notificar en 72 hores segons el RGPD. Els plans analitzen bretxes per evitar violacions.
- Per a cada àrea: actiu, bretxa possible, una mesura concreta, la llei implicada. Parteix de l'auditoria **passiva** del teu D5.
- Cada tipus nou de dades necessita el seu **tractament** definit al llarg del cicle de vida.
- Cada objectiu necessita un **indicador** (KPI) amb una fórmula i una font de dades que realment tens.
- La **integració** té tres capes: dades, aplicacions, plataformes. Cada dada té una **font de referència**, i les aplicacions es comuniquen per mitjà d'**API**.
- Pregunta sempre què passa si cau una peça: el 19 de juliol de 2024, una sola actualització defectuosa va aturar la facturació a l'aeroport de Palma.

Comprovació ràpida

1 Quina diferència hi ha entre una bretxa de seguretat i una violació de dades personals?

- **A** Cap: són dos noms per a la mateixa cosa
- **B** Una bretxa és un punt feble que es podria aprofitar; una violació és un incident que ja ha passat
- **C** Una bretxa només afecta l'OT i una violació només afecta l'IT
- **D** Una violació sempre la provoca un atacant extern

2 Quina d'aquestes mesures s'ajusta bé a una bretxa concreta?

- **A** «Instal·lar un antivirus a cada ordinador», per a totes les àrees
- **B** «Un compte per persona i MFA», per a un portal on el personal dels hotels comparteix una contrasenya
- **C** «Comprar un encaminador més ràpid», per als registres de temperatura en paper
- **D** «Contractar un advocat», per als dispositius IoT amb contrasenyes de fàbrica

3 Amb el web real de la teva empresa, quina d'aquestes accions es permet al projecte del curs?

- **A** Escanejar-ne els ports oberts per trobar serveis vulnerables
- **B** Provar contrasenyes habituals a la pàgina d'inici de sessió
- **C** Llegir-ne les capçaleres de seguretat a securityheaders.com i el bàner de galetes
- **D** Enviar-li un correu de pesca (phishing) de prova

4 Què fa que un indicador es pugui fer servir al pla?

- **A** Sona impressionant a la presentació
- **B** Mesura una cosa que no té relació amb els objectius, i per això és objectiu
- **C** Té una fórmula fixa i es pot calcular amb dades que el pla realment recull
- **D** Es calcula només una vegada, al final del projecte

5 Què és la font de referència d'una dada?

- **A** L'aplicació més cara de l'empresa
- **B** L'únic sistema on aquella dada es crea i es corregeix; els altres la copien d'allà
- **C** La còpia de seguretat al núvol
- **D** Qualsevol full de càlcul on aparegui la dada

6 En un diagrama d'integració, què hauria de dir cada fletxa?

- **A** Res: les fletxes només mostren que dues caixes estan relacionades
- **B** Què hi viatja i com: per exemple «comandes, per API»
- **C** El preu de cada aplicació
- **D** El nom de la persona que la va instal·lar

7 Un hotel fa servir un sistema de reserves al núvol connectat al sistema de claus de les portes. Quines dues preguntes hauria d'ajudar a respondre el seu diagrama d'integració?

- **A** Si el sistema de reserves cau, els hostes encara poden obrir les habitacions?
- **B** De quin color haurien de ser les caixes del diagrama?
- **C** Quin sistema té la llista correcta d'hostes, i com l'obté el sistema de claus?
- **D** Quantes plantes té l'hotel?

Les dades, les portes i les canonades ja hi són. Les darreres peces són les persones que gestionaran la nova ciutat i el pla escrit del que canvia i quan: Persones i documentació.

Solucions

1. B · El pla analitza les **bretxes** per evitar les **violacions**. I una violació també la pot provocar un error, com un correu enviat a la persona equivocada.

2. B · Una mesura ha de **tancar una bretxa concreta**. Les contrasenyes compartides es tanquen amb comptes personals i autenticació multifactor.

3. C · Només observació **passiva**: el que el web ja mostra a qualsevol visitant. Mai no escanegis, no sondegis ni intentis iniciar sessió a una empresa real.

4. C · Un **indicador** converteix dades en una comprovació d'un objectiu. Si les dades no són al teu diagrama, no el pots calcular.

5. B · Amb una sola **font de referència**, l'adreça del client es corregeix en un sol lloc i tots els altres sistemes reben la correcta. Amb diverses, es contradiuen.

6. B · Una fletxa sense contingut amaga la part important. Etiqueta **què** hi viatja i **com** (API, fitxer, a mà), així veuràs les friccions.

7. A, C · Les preguntes de control de qualsevol diagrama: **què passa si cau una peça**, i **on és la font de referència i com viatja la dada**.