sessió 3 RECORDEU QUE AIXÒ ÉS UN LLIURAMENT PER PERSONA, NO PER FER EN GRUP.
NOTA: els que heu fet cada treball no cal que contesteu les preguntes <u>del vostre treball</u>

09.- Privacitat al núvol.

- Si fossis un centre com la UPC, creus que seria més segur davant atacs de ramsomware tenir les dades a una companyia com les estudiades o a un CPD *on-premises*? Perquè?

En general, no hi ha una resposta única, ja que la seguretat depèn no només del model d'implementació, sinó també de com es configuren i gestionen els sistemes, les polítiques de seguretat implementades i la consciència i formació dels usuaris. En el cas de la UPC, preferiria jo mateix gestionar les dades en un CPD on-premises ja que el poder controlar la infraestructura sense una segona veu pot ajustar-se millor a les necessitats de la universitat.

- Com garanteixen les companyes estudiades la protecció de les teves dades?

Utilitzen tècniques estudiades a l'assignatura com la redundància (tant de dades com la línia elèctrica), encriptació de les dades, protecció d'amenaces internes a la empresa (limitar l'accés al personal), i el compliment de les lleis de seguretat generals.

- Sempre queda la "sospita" al posar les dades de la teva empresa i els teus clients en mans d'una d'aquestes empreses al núvol, que no facin servir aquesta informació per profit propi. Posa un exemple d'una companyia/ negoci/ institució/ servei que MAI posaríeu al núvol (i el tindríeu on-premises) i un altre exemple d'un que no sembli problemàtic de posar al núvol.

Informació que destapi les parts més dèbils de la seguretat de les empresa (com horaris, estat de les màquines...) o dades personals dels treballadors, contrasenyes i correus dels empleats són informació molt golosa i susceptible a atacs.

D'altre banda, informació estadística científica és totalment segura per a pujar al núvol, per exemple els percentatges d'on treballa la gent en Espanya, quantitat de morts per fumar, nombre d'escoles a una ciutat...

10.- Vulnerabilitats del núvol.

- Quines són les vulnerabilitats més habituals dels que t'has de preocupar si tens el teu propi CPD (on premises) i dels que et pots despreocupar si estàs al núvol?

A l'estar al núvol no t'has de preocupar per alguns perills físics com per exemple si hi ha un terratrèmol a prop de la teva zona de treball les dades estaran segures, o el mateix per inundacions.

Per altre part, estar al núvol sol ser més vulnerable a rebre ciberatacs i que hi hagin data leaks.

- De totes les coses que pots fer per prevenir aquestes vulnerabilitats, indica les dues que per tu serien les més importants si fossis el responsable dels serveis que té UPC al núvol.

Establir i gestionar de manera rigorosa els controls d'accés als sistemes i dades. Això inclou la implementació de polítiques de control d'accés granulars, autenticació forta, revisió regular d'usuaris i privilegis, i la implementació de pràctiques de mínims privilegis per garantir que els usuaris tinguin accés només al que necessiten.

Desplegar sistemes de monitorització continua que puguin detectar activitats anòmales o comportaments no autoritzats en temps real. A més, tenir un pla de resposta a incidents ben establert que permeti una acció ràpida en cas de detecció d'una amenaça o atac.

- Reflexió: si tens la teva empresa al núvol, cal un CISO? Quines funcions tindria?

Potser no caldria, però si hi hagués un CISO en una empresa amb operacions en el núvol tindria la responsabilitat de garantir que les pràctiques de seguretat siguin efectives i s'ajustin als requisits específics d'aquest entorn, protegint així les dades i els recursos empresarials contra amenaces de seguretat.

11.- Digital Services Act (DSA).

- Descriu amb les teves pròpies paraules (i en 4 línies com a molt) quin problema resol (o intenta resoldre) la DSA.

La DSA busca abordar els reptes emergents en el sector de pagaments en línia. Pretén millorar la seguretat de les transaccions electròniques i protegir millor als consumidors i comerciants contra pràctiques fraudulentes i altres amenaces en el context dels serveis de pagament digital.

- Un gran poder implica una gran responsabilitat. Penseu que aquestes plataformes tenen el deure de vetllar pels usuaris (per exemple, verificant informacions o vetant discursos d'odi) o la llibertat està per sobre de tot? (no és fàcil de contestar, ni hi ha respostes correctes, només vull que reflexioneu).

Jo simplement les veig com eines, com un martell o una serra, així que com menys condicions d'ús més llibertat creativa, sí que és veritat que és millor no passar-se de llibertat, però per a avançar penso que no s'haurien d'imposar massa límits.

- Una altra de reflexió: a la xarxa sembles anònim enfront d'altres usuaris, però les companyies coneixen perfectament qui ets. Si vosaltres tinguéssiu la capacitat de decidir, prohibiríeu els bots orientats a donar informació fake per influir en l'opinió pública (com les votacions del brexit o les eleccions als EUA)? Denunciaríeu davant les autoritats, i per iniciativa pròpia, les persones amb discurs d'odi, intent de manipulació o que difonen falsedats? (encara que sigui semblant és una pregunta molt diferent a l'anterior)

Com a persona molt científica i a favor del coneixement, em dóna molta ràbia quan es difundeix informació falsa o fraudulenta per a controlar a la gent menys espavilada, i em sap molt greu, per tant personalment prohibiria qualsevol tipus d'informació modificada o que no estigui verificada. Tot i que també penso que aquesta pràctica és una espècie de "filtre" per a saber qui és una persona que pensa per ella mateixa i qui simplement es deixa anar per les masses.

12.- Seguretat.

- Què fa un software tipus SIEM (Security Information and Event Management)? Quin tipus d'atac pot prevenir?

És un software que recopila, analitza i fa informes o proporciona solucions a la seguretat en general d'una empresa o dades. Pot prevenir atacs de tipus malware, DDoS, phishing o detectar activitats anòmales en el sistema.

- Què penses que és el més important davant els atacs de ramsomware, la prevenció o garantir la recuperació? Raona la resposta.

Depèn de a qué es dediqui la empresa, si manega molta informació crítica llavors el més important és garantir la recuperació d'aquesta, i si la informació és confidencial o molt important mantenir-la oculta per a la integritat de la empresa llavors la part que té més pes es la prevenció dels atacs.

- Reflexió: potser no he insistit prou en la importància de tenir un pla de contingència. ÉS IMPRESCINDIBLE. Escriu en poques línies com pots convèncer a un CEO que no entén d'informàtica la necessitat de tenir un pla de contingència.

Li diria algo com: "Imagina que el teu ordinador es veu afectat per un virus o tenim una fallada en els servidors. Sense un pla de contingència, això podria resultar en temps d'inactivitat i pèrdua de dades crítiques, amb conseqüències financeres **GREUS**. Amb un pla, estarem preparats per respondre ràpidament, minimitzar la interrupció dels negocis i protegir la integritat dels nostres sistemes. És una inversió vital per garantir la continuïtat i la resiliència del nostre negoci davant de possibles amenaces informàtiques."

Fent especial èmfasi en la part de pèrdues monetàries GREUS.