13.- Virtualització.

- Quins son els avantatges de fer servir virtualització? (breu, les més importants per a tu)

La eficiència al poder fer servir els recursos hardware d'una sola màquina física per tenir molts de màquines virtuals. Flexibilitat per tenir qualsevol sistema operatiu amb els recursos que vols a les màquines virtuals, sent una independent d'altra. També ofereix una migració (portabilitat) ràpida i fàcil.

- Descriu en poques paraules el funcionament d'un hypervisor.

És un software que fa d'intermediari entre el hardware i les VMs, repartint els recursos disponibles i assegurant-se que no interfereixen entre elles. Permet que una màquina física (host) presti suport a diverses màquines virtuals (guests) convidades mitjançant l'ús compartit virtual dels seus recursos, com la memòria i el processament.

- Reflexió: Suposem que les MV no comparteixen pràcticament dades i totes són locals. És més pràctic que les dades de cada MV estiguin al seu disc local, o tenir un disc centralitzat? Raonar.

Crec que ja que encara que no comparteixen quasi dades, és millor tenir-ho cada un al seu disc local, per si vull migrar-ho sigui més fàcil, i ho tindria tot en un lloc i ja. Al tenir-ho centralitzat si elimino un arxiu important no sabria a quina màquina virtual pertany.

14.- Monitorització.

- Indica 2 coses que es poden monitoritzar (escull quines 2) i indica quins problemes implica no monitoritzar-les

S'hauría de monitoritzar la seguretat, per possibles atacs i assegurar els nostres equips, i també monitoritzar els servidors, per si algun cau de sobte i poder solucionar-ho en poc temps.

- Les eines de monitorització són complementàries? Com penses que poden treballar juntes?

Entenc que sí, que es poden treballar junts ja que es poden enfocar en diferents coses, al haver-hi molts de tipus de monitorització (al pdf hi explica uns 5, els més generals), no hauria de tenir problema per "solapar-se".

- Reflexió. Penseu que la informació que s'extreu de software de monitorització com els vistos poden ser utilitzats pel CIO o el CEO per prendre decisions? Raona la resposta.

Potser per al CIO però no crec que per al CEO. La informació que s'extreu de la monitorització crec que seria més interessant per als tècnics i que aquests prenguin decisions més que al CIO, però clar, el CIO és el "cap".

15.- Eines d’orquestació.

- Quina és, per a tu, la funció de les eines d’orquestració que fan que siguin realment útils (escull una i raona)?

Poder configurar (entre altres funcions) molts de servidors a la vegada, amb un script, incrementant fiabilitat, flexibilitat i reduint temps d’anar configurant cada servidor manualment un a un. També quan s'actualitzen programes i gràcies a les eines d’orquestració no hem d’estar comprovant tot el temps.

- De les eines presentades, quina t’ha sorprès? Per quina funcionalitat?

M’ha sorprès Terraform, per les etapes de vida que té, que funciona com si fos una màquina virtual, on inicialitzes, fas el que has de fer, i com a últim pas la pots destruir per alliberar recursos.

- Reflexió, les eines d’orquestració semblen tenir molt futur, però van evolucionant. Reflexiona sobre quines coses es poden anar automatitzant i formar part de les coses que fan els orquestradors.

Com aquestes eines ens ajuden d’una forma sense intervenció humana, que ens proporciona molts d'avantatges com la fiabilitat, perquè els humans podem causar més errors que un script ben fet, es podria per exemple executar no solament scripts als casos que es fan servir ara i fer servir-los en més coses, com una reparació de bugs en codis, o experimentar tests amb elles.

16.- Seguretat.

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

Un SIEM és un sistema de seguretat que centralitza l'emmagatzemament i la interpretació de les dades rellevants de la seguretat, així tenint un control total de tots els events que succeeixen. La majoria tenen les mateixes funcionalitats bàsiques: gestió de registres, correlació d'events i anàlisis, i monitorització d'incidents i alertes de seguretat.
Es suposa que genera una protecció contra tot tipus d'amenaces i atacs, com malware, ransomware, denegació de serveis (DoS), phishings, worms, etc.

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

Ambdues són importants, però crec que garantir la recuperació, ja que encara que passa l'atac pots recuperar totes les dades en un temps (que hauria de ser petit). Sempre hi haurà una manera d'atacar i no pots prevenir al 100% (encara que ha de ser alt aquest percentatge) però si el teu sistema de recuperació és bona tindràs les teves dades una altra vegada almenys. Ara, com és ransomware, estaria bé que la gent tingui un poc més de cura amb mails o arxius sospitoses.

- 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.

Com no entén d'informàtica hauríem d'explicar-li que no tenint un pla de contingència podria costar-li a la empresa molts de diners en cas de que hi hagi un atac, i és millor prevenir-ho.