W18D4 – perdita annuale di un'azienda.

Esercizio obbligatorio ed esercizio facoltativo.

ALE, ossia annualized loss expectancy, indica il valore della perdita subita da un'azienda nell'arco temporale di un anno in caso di disastro e si calcola moltiplicando il valore della single loss expectancy, SLE, cioè la perdita che si subisce al verificarsi di un disastro per il numero delle volte in cui si stima che si possa verificare quell'evento disastroso in un anno (ARO). In questo modo si ha la formula ALE=SLE x ARO. SLE si calcola moltiplicando l'exposure factor EF, cioè la percentuale di asset che verrebbe impattata da un certo evento disastroso e il valore dell'asset (AV), per cui si ha SLE=AV x EF. Per questo motivo, ai fini dell'esercizio calcolerò prima il valore della single loss expectancy SLE con AV x EF, e poi calcolerò l'annualized loss expectancy ALE con SLE x ARO.

Caso 1: Inondazione sull'asset "edificio secondario". SLE=150.000 x 0,4 =60.000. ALE=60.000 x 0,02 = 1200 euro all'anno. L'impatto sulla compagnia in caso di questo disastro è quindi di 60.000 euro quando l'evento si verifica e di 1200 euro all'anno.

Caso 2: terremoto sull'asset "datacenter". SLE=100.000 x 0,95= 95.000. ALE=95.000 x 0,03= 2850 euro all'anno. L'impatto di un terremoto sul datacenter è di 95.000 euro se si verifica l'evento e di 2850 euro all'anno.

Caso 3: incendio sull'asset "edificio primario". SLE =350.000 x 0,6= 210.000. ALE=210.000 x 0,05= 10.500 euro/anno. Se si verifica un incendio nell'edificio principale, i danni ammontano a 210.000 euro con una perdita annua di 10.500 euro all'anno.

Caso 4: incendio sull'asset "edificio secondario". SLE=150.000 x 0,5= 75.000 euro. ALE=75.000 x 0,05 = 3.750 euro/anno. Un incendio nell'edificio secondario causa 75.000 di perdite e 3.750 euro all'anno di perdita.

Caso 5: inondazione sull'asset "edificio primario". SLE=350.000 x 0,55= 192.500. ALE=192.500 x 0,02= 3.850 euro/anno. L'impatto sulla compagnia di questo evento è di 192.500 euro, con una perdita annua di 3.850 euro all'anno.

Caso 6: terremoto sull'asset "edificio primario". SLE=350.000 x 0,8= 280.000. ALE=280.000 x 0,03= 8.400 euro/anno. Con un terremoto che colpisce l'edificio primario ci si aspetta una perdita di 280.000 euro e una perdita di 8.400 euro all'anno.

La triade CIA, ossia Confidentiality, Integrity ed Availability indica dei principi fondamentali per valutare la sicurezza dei dati e di un ambiente informatico. Confidentiality, ossia riservatezza, è un principio che prevede che l'accesso ai dati sia dato solamente a chi è autorizzato ad accedervi. Deve essere quindi mantenuta la riservatezza del dato, evitando accessi non autorizzati tramite tecniche di cifratura o di controllo degli accessi. Integrity, ovvero integrità, si riferisce al mantenimento dell'affidabilità e della correttezza dei dati, per evitare che avvengano delle modifiche non autorizzate ai dati e che il dato arrivi inalterato dal mittente al destinatario. Si possono usare funzioni di hash o checksum per verificare l'integrità del dato. Infine, Availability indica la disponibilità del dato che, deve essere sempre

disponibile anche in un momento di crisi per i soli utenti autorizzati. La disponibilità va garantita sia in caso di disastri naturali, sia in caso di problemi tecnologici e servono quindi tecniche anti denial of service, backup e ridondanza per mantenere il dato sempre disponibile. Immaginando lo scenario di un terremoto nel datacenter, le minacce alla confidenzialità, all'integrità e alla disponibilità dei dati possono essere molte e di grave impatto. Per quanto riguarda la confidenzialità, un terremoto potrebbe danneggiare seriamente l'edificio e consentire l'accesso fisico ai dati da parte di persone non autorizzate e con degli hardware spostati o danneggiati diventa ancora più facile per un malintenzionato avere accesso alle informazioni. Anche un danneggiamento fisico dei server o dei dischi nei quali sono contenuti i backup rende più agevole l'accesso dei dati a personale non autorizzato, andando a minare la confidenzialità dei dati. Anche l'integrità dei dati è minacciata, perché il danneggiamento fisico di hardware o server e le possibili interruzioni nella fornitura della corrente potrebbero arrivare ad alterare o addirittura far sparire dei dati. Eventuali copie dei dati, per esempio in un backup o in sistemi replicati, potrebbero venire alterate a causa del disastro e l'accessibilità del datacenter a causa dei danni alla struttura potrebbe consentire accessi non autorizzati per l'alterazione dei dati. Anche la disponibilità dei dati viene messa seriamente in pericolo da un terremoto in un datacenter, perché potrebbero essere danneggiate seriamente le strutture hardware o i server, impedendo il recupero dei dati. Potrebbero essere distrutte le infrastrutture di rete con il conseguente isolamento del datacenter ed anche le interruzioni della corrente elettrica rappresentano un pericolo per la disponibilità dei dati. Per proteggere la confidenzialità dei dati anche in caso di terremoto è opportuno verificare che possa essere mantenuto un certo livello di sicurezza fisica anche dopo un evento simile, ad esempio mantenendo dei sistemi di videosorveglianza e delle verifiche agli ingressi e trovare delle soluzioni per fare in modo che eventuali copie di backup fisiche non si trovino proprio nel datacenter, a disposizione di malintenzionati che possono andare a prelevarle dopo il terremoto. È utile anche accertarsi che i dati siano criptati sia in transito, sia nei server e nei database, affinché un malintenzionato nel datacenter li trovi illeggibili e inutilizzabili. Per difendere l'integrità dei dati anche in caso di un terremoto, serve avere una chiara politica di backup che preveda anche una certa ridondanza ed utilizzare funzioni come hash o checksum per poter verificare in ogni momento che l'integrità dei dati sia stata mantenuta. Per garantire la disponibilità dei dati è necessario elaborare e saper implementare un disaster recovery plan, che includa una certa ridondanza nella generazione della corrente elettrica, ad esempio tramite dei generatori aggiuntivi in caso di disastro, una ridondanza fisica con più dischi o più server per rispondere ad una crisi e dei sistemi di backup anche su cloud. Questo dovrebbe aiutare a rendere i dati sempre disponibili anche in caso di un terremoto nel datacenter.