

Exercise: Identify a RISK and a RISK owner

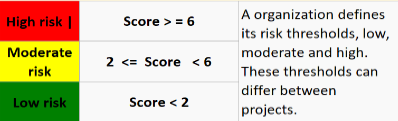
Det ville være rart at have mere information omkring virksomhedens gøren, til bedre at kunne analysere hvilke risici virksomheden står overfor.

Men på baggrund af at virksomhedens medarbejdere alle skal tilgå databasen gennem en internet browser, mener vi at versions control er en af de mere relevante risici

* Social Engineering/ “Over the shoulder” loss of information to visiter / colleague - **P1**
* Email scams/Phishing (Keylogger/Malware) - **P2**
* Remote access til database web page; spoofing - **P3**
* ikke segmenteret database og ingen info om backup - **P4**
* Software håndtering og rettigheder. - **P5**
* Downgrade / MITM
* risiko ved at have outsourcet database, “ mister kontrol og evt udbyder ikke er up to date sikkerheds wise”
* GDPR personal data opbevaret potentialt ukendt placering ?
* Password politikker og generelle retningslinjer
* Monitorering af bruger aktivitet / test af om en bruger kan hvad de skal / mere / mindre



| Probability | Threats | | | |
| --- | --- | --- | --- | --- |
| High  3 | 0 | 3 | 6 | 9 |
| Moderate  2 | 0 | 2 | 4 - **P2** | 6 - **P1 , P4** |
| Low  1 | 0 | 1 | 2 - **P5** | 3 - **P3** |
| Very low  0 | 0 | 0 | 0 | 0 |
| Impact | Very Low 0 | Low 1 | Moderate 2 | High 3 |



**P1** placeres som moderat probability og high i konsekvens, mere info omkring virksomhed krævet i forhold til hvor godt de informere / uddanner deres medarbejderer i sikring fra social engineering, samt om der er lagt tanke bag hvor kontoret er placeret og hvordan bygningen er segmenteret i forhold til brugere og brugerrettigheder.

**P2** ,Et business firma der har et højt antal mais ind og ud , har en øget chance for at der kommer en phishing mail igennem, dog kommer dette ned til at hvor sofistikeret denne mail er bygget

**P3**, Vi antager, at man kun kan få adgang til databasen på firmaets lokale internet, hvorfor vi har sat sandsynligheden til at være 1 - Low. Hvis hackeren får adgang til databasen, vil det have store konsekvenser for firmaet (High - 3), idet hackerne får adgang til alle firmaets confidential data, herunder personlige data, strategier og business economy.

**P4 .** Hvis virksomhedens data går tabt er det katastrofalt, hvis der ikke forekommer en backup, og vi får ingen information omkring denne.

**P5 ,** Det kan have medium til high konsekvenser hvis virksomheden anvender outdatet versioner samt styring af brugerrettigheder



Vi vurdere at virksomheden har gjordt et fornuftigt forsøg på at sikre virksomhedens følsomme data gennem styring af brugerrettigheder, dog er der nogle steder virksomheden væsentligt kan forbedre.

Backup er en væsentlig ting som virksomheden skal være opmærksom på at anskaffe sig, eller gøre overvejelser over. dette er en tikkende bombe og virksomheden gør klogt i at priotere at få håndteret dette.

Social engineering og spearfishing approaches vil være en god ide for virksomheden at uddanne deres medarbejder i hvis det ikke er en ting de gør i forvejen.



A.8.1 Ansvar for aktiver.

A.9.2 Administration af brugeradgang.

A.9.4 Styring af system- og applikationsadgang.

A.12.3 Backup

A.12.4 Logning og overvågning.

Dette vil være en god ide at have med pga mængden af medarbejdere der alle har adgang til databasen.



**Damage control:**

Luk adgang til database, så hackere eller ikke nødvendigt personale får adgang og sørg for at hændelsen bliver stoppet.

Check logs for trafik/ramte områder.

* Luk porte
* Whitelist/blacklist

Luk adgang til ramte brugerkonti

**Recovery:**

Kør backup

* 3, 2, 1
* Patche og lukke sikkerhedshuller
* Lukke/åbne servere, Dockers cluster, micro-services

**Communication:**

Intern kommunikations channel i tilfælde af breach

Advar kolleger, kunder

72-timers kontakt til datatilsyn

