IT Sikkerhed

OPGAVE B: Sikkerhedsanalyse af sociale medier

Kasper Passov pvx884

Contents

1 Resumé af firma og system

1.1 Firmaets risiko niveau

Firmaet BIOmedix er et firma med høj sårbarhed overfor informations tyveri. En lækage af forsknings resultater kan have meget alvorlige konseknverser for BIOmedix, da salg af disse resultater og patenter der er kommet deraf er deres primære inkomstkilde. Dette betyder IT sikkerheden bør være i firmaets fokus for at beskytte disse aktiver.

1.2 Resumé af det nye system

Der skal indføres fire nye sociale medier i BIOmedix. Dette har jeg valgt at dele op i 2 grupper.

Eksterne systemer Den ene er 3 sider i de sociale netværker Facebook, Twitter og LinkedIn som jeg vil kalde de eksterne systemer, idet pointer med disse er at give firmaet en mulighed for at kommunikere med folk udenfor firmaet. Jeg har valgt at samle disse systemer i en gruppe da jeg mener der er mange ligheder i hvilke trusler og sårbarheder disse systemer bliver udsat for, og derigennem skal sikkerheden i disse systemer håndteres ens. Kodeord og brugernavne til disse kontoer bliver holdt af kommunikationsafdelingen, som står for opdateringer.

Internt system Det sidste system, Yammer, er et lukket socialt netværk for alle firmaets ansatte. Systemet lader dem blandt andet opdatere arbejdsstatus og danne projektgrupper. Jeg vil referer til dette netværk som et internt system, da mange af de trusler og sårbarheder Yammer er udsat for ville kunne bruges på lignende systemer i fremtiden.

2 Aktiver

2.1 Eksterne systemer

Vores vigtigste aktiv i de eksterne systemer er muligheden for at videregive information til den bredere befolkning.

2.2 Interne systemer

Informationen på det interne system Yammer skal beskyttes fra udekommende, da der vil være store mængder af kritisk information på dette netværk. Derudover skal ansatte have nem og hurtig adgang til information, gerne hvor som helst og når som helst.

2.3 Begrundelse for aktiver

Spredning af information De eksterne systemers primære funktion er at give firmaet en kommunikations kanal til den brede befolkning. Dette kan både være en nyhed om et gennembrud, et opslag til en ny stilling eller general information om firmaet. Denne aktiv skal beskyttes ved at holde kommunikations linjen åben og så uhindret som mulig.

Information på det interne system Yammer kommer til at indeholde hvad de ansatte arbejder på, hvem de arbejder med, forskningsidéer og filer. Et brud på dette netværk vil blotte alt information BIOmedix har, og gøre det muligt for konkurrenter eller patenttrolde at se hvor langt BIOmedix er med et stykke forskning, og muligvis presse en patent frem inden BIOmedix kan færdiggøre sig.

Adgang til Yammer Uden de ansattes adgang til Yammer, vil dette cloud system ikke være sikkerheds risikoen værd. Derfor skal det gøres så nemt som muligt for de ansatte at få adgang til Yammer, gerne både på arbejdspladsen og i hvert ansats hjem.

3 Sikkerhedsmål

Internt Et sikkert system der lader ansatte dele information nemt og hurtigt hvor som helst og når som helst.

Eksternt Et system der lader firmaet snakke og dele information med den bredere befolkning, for f.eks. at finde dygtige medarbejdere og for at reklamere for udviklinger lavet.

4 Trusselsaktører

Internt: Hackere (Utilfredse ansatte)

Eksternt: Konkurenter Hackere (Utilfredse ansatte)

5 Trusler

Internt:

Udbyder leaker passwords Ansatte mister passwords

Eksternt:

Udbyder Leaked passwords Ansatte mister passwords

5.1 Relevante angreb

5.1.1 AP's Twitter-konto

Angreb

Figure 1: Tweeten fra hackeren over nyhedsbureauet Associated Press [1]

Relevans for BIOmedix Et sådan angreb kan fjerne tilid og lade konkurrenter samt ondsindede hacker sprede misinformation in BIOmedix navn

5.1.2 LinkedIn password-lækage

Angreb

Relevans for BIOmedix Et stort leak af passwords fra en sådan side kunne betyde alle BIOmedix' sociale medie sider ville være usikre, hvis det samme password var brugt overalt. Kig information igennem for ændringer, og skift password. SØRG FOR DER ER FORSKELLIGE PASSWORDS TIL ALLE SIDER DER BRUGER SAMME MAIL!

6 Sårbarheder

Ansattes password styrke. Kritisk information er ikke på firmastyret servere.

7 Modforanstaltninger

Password styrke og brug

8 Risici

9 Foreslåede modforanstaltninger

10 Konklusion

References

[1] www.businessinsider.com/ap-hacked-obama-injured-white-house-explosions-2013-4

[2] www.guardian.co.uk/business/2013/apr/23/ap-tweet-hack-wall-street-freefall