**Eigandi: Daníel Þór Ingólfsson**

**Verkefni - Introduction to Cybersecurity**

1. Útskýrið með eigin orðum eftirfarandi hugtök sem tengjast upplýsingaöryggi:
   * **Availability**

**Eða framboð, er það hugtak sem notað er í netöryggi yfir það að það sé alltaf hægt að tengjast og ná í þá sem tryggja öryggið okkar.**

* + **Confidentiality**

**Eða trúnaður, er orð sem er notað til að hughreysta fólk um að það sem það sendir frá sér, fari ekki til neins annars nema þess sem er sent á.**

* + **Integrity**

**Heiðarleiki, er notað þannig að fyrirtæki fullvissa fólk um það að enginn fikti í neinu sem fer í gegnum þá og efninu sé skilað á réttan áfangastað.**

1. Nefnið þrjár mismunandi gerðir af hökkurum og tilgreinið muninn á þeim.

Til eru þrjár tegundir af hökkurum, hvíthattar, svarthattar og gráhattar. Hvíthattar eru þeir hakkarar sem að brjótast inn í gagnagrunna til þess að finna veikleika og láta vita til þeirra sem unnið er fyrir ef eitthvað kemur upp. Svarthattar eru alræmdir glæpamenn sem svífast einskis til að stela upplýsingum og nýta þær í glæpsamlegum tilgangi. Síðast en ekki síst eru það gráhattarnir. Þeir eru hvorki alveg hvítir eða svartir. Þess vegna eru þeir eitthversstaðar á milli, þar að segja þeir hakka stundum inn og láta svo vita á eftir, en stundum taka þeir krimmann á það og stela upplýsingum.

1. Flokkun á ófullkomnu netöryggi (e. categorizing security vulnerabilities) er:

* **Weaknesses in security practices**

**Þar sem fyrirtæki ættu ekki að búa til sín eigin öryggisforrit, heldur nota eitthvað sem hefur verið prófað og reynt á.**

* **Access-control problems**

**Er það að stjórna því hver fær aðgang og hver ekki og það mistekst.**

1. Til eru nokkrar gerðir af spilliforritum(maleware). Tilgreinið hvað hvert spilliforrit gerir og hvernig það virkar.

* **Spyware**

**Er búið til að njósna og fylgjast með notanda. Gerist oft að það breytir öryggisstillingum.**

* **Adware**

**Auglýsinga forrit sem er gert til að sjálfkrafa koma með auglýsingar, kemur oft með Spyware.**

* **Bot**

**Illt forrit sem er búið til að gera eitthvað á netinu sjálfkrafa. Oftast skaðlaus en geta verið notuð í vondum tilgangi.**

* **Ransomware**

**Er gert til þess að halda kerfi sem það er notað á föngnu, þangað til að til dæmis greiðsla er greidd.**

* **Scareware**

**Er forrit sem er gert til að hræða notanda í að gera eitthvað sem endar bara illa fyrir hann. Býr til skjái sem líta næstum nákvæmlega eins út og á innra kerfinu sjálfu.**

* **Rootkit**

**Er notað á kerfi til þess að búa til bakdyr á það svo hægt sé að komast inn þegar viðkomandi vill.**

* **Virus**

**Vírus er notaður eiginlega alltaf i illum tilgangi og er festur mjög oft við skjöl eða forrit sem eru í fullkomnu lagi.**

* **Trojan horse**

**Tróju hestur er það sem er notað til að að laumast inn í kerfi og gera illar breytingar á því.**

* **Worms**

**Eru illgjarnir kóðar sem afrita sig sjálfir með því að notfæra sér veikleika í kerfi sjálfstætt.**

* **Man-In-The-Middle (MitM)**

**Maðurinn í miðjunni er það sem leyfir árasar manninum að taka stjórnina á tæki án þess að eigandinn taki eftir. Með þeim aðgangi getur hakkarinn stolið notanda upplýsingum, áður en þær halda á sinn upprunalega stað.**

1. Hvaða áhrif hefur það á tölvuna að vera sýkt af spilliforrit. Nefnið nokkur dæmi

Dæmi um það sem getur gerst við tölvuna er að CPU notkun getur hækkað, tölvan hættir að virka í tíma og ótíma, gögnum er eytt og óþekkt forrit eru gangsett.

1. Til að komast yfir Wi-Fi lykilorð eru notaðar eftirfarandi aðferðir:

* **Social engineering**

**Er aðferð sem ýtir við fólki í að deila og gera eitthvað við persónulegar upplýsingar. Þeir sem nýta sér þessa aðferð reyna oftast að vinna á hjálpsemi og góðvildar fólks.**

* **Brute-force attacks**

**Þegar að hakkararnir nota alla mismunandi möguleika til að finna út lykilorðin, og notast þeir oftast við sérstök forrit sem sérhæfa sig í því.**

* **Network sniffing**

**Er þar sem hakkarar hlusta og fylgjast með því sem er sent frá netinu getur viðkomandi fundið aðgangsorð sem eru send í skýrum texta, þó að aðgangsorðin séu þó dulkóðuð geta þeir ennþá brotist inná þau.**

1. Hvað er átt við með hugtakinu „Phising“?

Er þegar illgjarn hópur sendir dulbúin tölvupóst með undirliggjandi fyrirætlunum, sem lítur út fyrir að vera frá traustverðum aðila og biður um persónulegar upplýsingar, svo sem fjárhagslegar eða aðrar.

1. Hvernig leita hakkarar að veikleikum í tölvukerfum?

Þeir kynna sér kerfið fyrst, taka síðan mikilvægar upplýsingar og leita svo að þekktum veikleikum að stýrikerfinu. Þegar veikleikinn er fundinn, leitar hakkarinn að eldri notfærslum fyrir veikleikann. Ef enginn er til, getur hann skrifað sína eigin.

1. Hvað er DoS árás og hvernig eru þær frábrugnar DDos árásum?

Er tegund netárásar og getur valdið eitthverri truflun á nettengingu notanda, tækja og forrita. DDos er svipað og DoS en kemur frá mörgum aðilum, en ekki bara einum.

1. Hvað er blönduð árás (e. blended attack)?

Blandaðar árásir nota alls konar tækni til að komast yfir upplýsingar. Þær vinsælustu senda fullt af ruslpósti, sjálfkrafa skilaboðum eða nota viðurkenndar vefsíður til að dreifa tenglum sem eru notaðir til að niðurhala í leynd Spyware og fleiru.

1. Hvernig er best að verja tölvuna fyrir utan að komandi árásum (nefnið 3 til 4 atriði)?

Vera með eldvegg á, nota Antivirus eða Antispyware, sjá um tölvuna og vernda öll tæki.

1. Hvaða eiginleika hefur gott lykilorð?

Engin nöfn eða orðabókarorð, engin tölvunöfn eða aðgangsnöfn, með sérstökum stöfum og 10 stafir eða meira.

1. Af hverju er gott að afrita gögn (e. back up)?

Það getur verið gott ef að harði diskurinn klikkar eða tölvan sjálf. Getur líka verið gott ef að þau eru stolinn eða dulkóðuð.

1. Hvað er tvíþætt auðkenni (e. two factor authentication)?

Er aukið öryggi fyrir innskráningar til þess að reyna að koma í veg fyrir innbrot. Tvíþætt auðkenning virkar þannig að maður skráir inn venjulegar upplýsingar og svo þarf maður að setja inn aðrar upplýsingar til að komast inn.

1. Hvað er OAuth (e. Open Authorization)

Er opið ferli sem leyfir notanda að nota þriðja aðila forrit án þess að gefa upp aðgangsorð.

1. Hvað er átt við með private browsing og hvernig stillir þú Google Crome vafran ef þú vilt nýta þér private browsing?

Private browsing er það sem er farið í til að fela sögu vafrans og koma í veg fyrir sumar rakningur á vöfrum. Dæmi um private browser í t.d. Chrome, heitir hann Incognito. Hægt er að kveikja á því með því að ýta á punktana þrjá uppi í hægra horninu og ýta á „new incognito window“.

1. Af hverju er mikilvægt fyrir fyrirtæki að fræða starsfólk sitt um netöryggi?

Vegna þess að ef það er ekki gert getur fyrirtækið orðið veikt fyrir netárásum ef starfsfólk notar kerfi þess og fær t.d. vírus inn. Þá getur fyrirtækið lent í miklum vandræðum.

1. Útskýrið hvað „Cyber Kill Chain“ er.

Er öryggisforrit sem greinir og leysir úr öryggis atvikum.

1. Útskýrið hvað „Security Playbook“ er.

Er samansafn af endurteknum skýrslum gagna uppspretta í fyrrverandi öryggisatburðum sem leiða til atvika greiningu og svörum. Tilgangur þessa er að greina tæki með illgjörn forrit og margt fleira.