**Verkefni - Introduction to Cybersecurity**

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

Availability (fáanleiki) er tryggt með því að stranglega viðhalda vélbúnaði og stýrikerfum. Ef vélbúnaður eða stýrikerfi bilar þá er viðgerðir gerðar strax við fyrsta tækifæri. Viðhalda þarf líka gögnum bæði með því að gera afrit reglulega af öllum gögnum og notkun á RAID (Redundant Array of Independet disks) stöðlum. Fáanleiki er líka tryggður með því að veita góða bandvídd til þess að koma í veg fyrir flöskuhálsi(Bottleneck)/þrengslum.

* + **Confidentiality**

Ráðstafanir gerðar til þess að tryggja friðhelgi notanda og veitanda. Friðhelgi notandans getur verið dulkóðuð til þess að koma í veg fyrir að viðkvæmar upplýsingar komist í vitlausar hendur. Fyrirtæki þurfa stundum að þjálfa starfmenn í öruggri/almennri skynsemi á lykilorðum og dulkóðun á gögnum og aðgangstýringu til þess að koma í veg árásir á friðhelgi starfmannsins og fyrirtækisins

* + **Integrity**

Aðferðir og ráðstafanir gerðar til þess að koma í veg fyrir að gögn skemmist. Gögn mega ekki breytast þegar er verið að afrita, þegar er verið að flytja gögn frá veitandanum til notandans og með vörnum gegn óviðkomandi einstaklingum. Checksum er notað til þess að bera saman gögn vara netþjóninum og á aðal netþjóninum ef t.d. það verðu tímabundið rafmagnsleysi eða ef netþjónninn hrynur.

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

**Hvít Hattur** er hakkari sem er ráðin sem verktaki eða starfsmaður hjá fyrirtæki. Hann/hún vinnur með fyrirtækinu í að finna öryggisgalla í kerfinu sem þarf að laga.

**Grá Hattur** er blanda af hvítum og svörtum hakkara. Grá hattar leita oft varnarlausum svæðum hjá netþjóninum án þess að vera með leyfi til þess. Þeir ráða síðan sjálfir hvað þeir gera við þær upplýsingar: annaðhvort láta þeir fyrirtækið vita (stundum fyrir pening) eða birta upplýsingarnar opinberlega á netinu.

Svart Hattur er hakkari sem notar hæfileika sína til þess að fyrir sinn eigin hagnað. Þeir eru þekktir fyrir að forrita vírusa og taka niður netþjóna. Svart hattar geta verið bæði byrjendur eða reynsluboltar.

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

* **Weaknesses in security practices**

Það er betra á að nota vel prófuð og viðurkennd öryggiskerfi í stað þess að forrita sitt eigið sem hefur aldrei verið prófað.

* **Access-control problem**

Þegar ó/þjálfaður starfsmaður hefur aðgang að gögnum og skjölum sem hann/hún ætti ekki að hafa aðgang að.

Útskýrið ofantalda veikleika í kerfunum.

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

* **Spyware**

Njósnaforrit sem stelur viðkvæmum upplýsingum og internet notkun án vitneskju notandans

* **Adware**

Auglýsingaforrit sem veitir reiðufé til eigandans með því að sýna auglýsingar á annaðhvort stýrikerfinu eða t.d. Google Chrome vafra hjá fórnarlambinu.

* **Bot**

Forrit hannað til að haga sér eins og manneskju á vissan hátt. Er notað mikið á t.d. Stefnumóta síðum og á félagsmiðlum

* **Ransomware**

Ransomware er vírus sem að tekur tölvu gíslingu með því að dulkóða allar gögn og skrár. Oft þarf að borga ákveðna upphæð til þess að fá gögnin sín aftur.

* **Scareware**

Spilliforrit sem að hræðir notandann til þess að kaupa forrit sem ætti að laga hættuna sem er ekki til staðar

* **Rootkit**

Samansafn af forritum hönnuð til þess að veita aðgang að tölvu eða stýrikerfi sem var áður ekki hægt.

* **Virus**

Spilliforrit sem að endurskapar sig með því eða endurstilla kóðan í forritum og setja í staðinn sinn eigin.

* **Trojan horse**

Spilliforrit sem að felur viljandi sanna tilgang forritsins.

* **Worms**

Spilliforrit sem að virkar eins og vírus nema að hann getur endurskapað sig án þess að fá aðstoð frá manneskju

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

Gerir árásarmanninum kleift að stjórna tölvuna/kerfið án þess að notandinn verði var við því

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

Spilliforrit geta hægt töluvert á tölvunni, sett upp forrit sem að notandinn vill ekki og gert hluti eins og t.d. slökkva á tölvunni eða álíka skipanir án leyfi frá notandanum.

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

* **Social engineering**

Aðferðir til þess að plata notandann til þess að veita árásarmanninum viðkvæmar upplýsingar með því að t.d. fá notandann til þess að ýta á hlekk sem spyr síðan notandann um viðkvæmar upplýsingar

* **Brute-force attacks**

Aðferð sem felur í sér að ofhlaða Wi-Fi Router af lykilorðum í von um það að eitt lykilorðið sé rétt.

* **Network sniffing**

Þjófnaður eða hlerun á netvirkni með forriti sem er kallað “sniffer”. Sniffer getur gripið svokallaða netpakka (network packets) og lesið þá ef þeir eru ekki dulkóðaðir

**Útskýrið hverja aðferð fyrir sig.**

1. **Hvað er átt við með hugtakinu „Phishing“?**

Phishing er svik samleg aðferð til þess að ná viðkvæmum upplýsingum frá fórnarlambinu með því að dulbúa sig sem treystandi vefsíðu, manneskju í email samskiptum og fleira..

1. **Hvernig leita hakkarar að veikleikum í tölvukerfum?**

Með því að nota t.d. social engineering eða phishing.

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

Dos áras (Denial of Service) er árás miðuð á tölvukerfi sem að tímabundið neitar eigundum/notendum aðgang. DDos árás notar margar tölvur í staðinn fyrir eina til þess ná sama markmiði og DoS árás sem notar bara eina tölvu.

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

Blended Attack (Blönduð árás) notar fleiri en eina aðferð t.d. trojan, worm og vírus til þess að komast inní tölvukerfi.

1. **Hvernig er best að verja tölvuna fyrir utan að komandi árásum (nefnið 3 til 4 atriði)?**
2. **Hvaða eiginleika hefur gott lykilorð?**

Gott lykilorð þarf að minnsta kosti 1 hástaf, 1 tölu, 1 merki(!”#$) og þarf að vera að minnsta kosti 12 stafir að lengd.

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

Ekkert er eilíft, Harði diskar og SSD diskar endast bara ákveðið lengi áður en þeir eru ónýtir. Gott er að taka líka afrit af gögnum ef að t.d. eigandinn missir harða diskinn sinn og hann skemmst.

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

Tvíþætt auðkenni byður notandan um lykilorð og sendir síðan t.d. póst til notandans sem biður notandann um leyfi til þess a skrá sig inn á vefsvæðið. Þetta er ein af mörgum álíka aðferðum

1. **Hvað er OAuth (e. Open Authorization)**

OAuth, leyfir þriðja aðila að nota opinberar (nafn, aldur, land og fleira) upplýsingar með því að nota svokallað token(lykil) án þess að birta lykilorð eða viðkvæmar upplýsingar t.d. á facebook eða “sign in with google”

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

Private browsing geymir ekki vafrarkökur né notandasögu en felur ekki ip töluna þína. Hægt er að nota Ctrl + Shift + N flýtileiðina til þess að fara í private browser á Google Chrome og á flestu vöfrum.

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

Ef að starfsólk þekkir ekki grunnreglur í netöryggi, getur hann dottið gildur hjá hakkaranum án þess að reyna það og afjúpað tölvukerfið.

1. **Útskýrið hvað „Cyber Kill Chain“ er.**

Cyber Kill chain eru 8 skref sem eru notuð til þess að reka til baka uppruna og aðferðir sem að hakkarar notuðu í netárás til þess að komast inn í tölvukerfið. Hugtakið á upprunan sinn frá Lockheed Martin.

1. **Útskýrið hvað „Security Playbook“ er.**

Samansafn af reglum og stöðlum hjá fyrirtæki sem að allir starfsmenn þurfa að þekkja. Security laybook á að veita starfsmönnnum skýra þekkingu á ábyrgð þeirra gagnvart fyrirtækinu og hvað á að gera þegar netárás er um að ræða.