**Svar úr Cyber security. -Þorvaldur Daði**



* Confidentiality: Annað hugtak um trúnað væri friðhelgi einkalífs. Stefna fyrirtækisins ætti að takmarka aðgang að upplýsingunum fyrir viðurkenndu starfsfólki og tryggja að aðeins þeir viðurkenndu einstaklingar skoði þessi gögn.
* Availability: Að kerfið sé 100% í lagi.
* Integrity: Það er nákvæmni, samkvæmni og áreiðanleiki gagna meðan á líftíma þeirra stendur.



* Hvítur hattur er siðferðilegur tölvuþrjótur.
* Grár hattur (gráhattur eða gráhattur) er tölvuþrjótur eða tölvuöryggissérfræðingur sem getur stundum brotið lög eða dæmigerð siðferðileg viðmið, en hefur ekki þann illkvittni sem er dæmigerður fyrir tölvuhakkara.
* Svart hattur (tölvuöryggi), tölvusnápur sem brýtur gegn tölvuöryggi af litlum ástæðum umfram illsku eða í eigin þágu.



• Hægt er að verja bæði kerfið og viðkvæms göngin með aðferðum eins og auðkenningu, heimild og dulkóðu.

• ferlið við að stjórna því hver gerir hvað og er allt frá því að stjórna líkamlegum aðgangi að búnaði, ákveða hver hefur aðgang að einhverjum auðlindum.



• Njósnaforrit er hönnun til að rekja og njósna um notandann.

• Auglýsingavörn er það sem nafnið á við, það er studdur hugbúnaður sem er hannaður til að birta auglýsingar sjálfkrafa.

• Bot er spilliforrit sem er hannað til að framkvæma aðgerðir sjálfkrafa, venjulega á netinu.

• Ransomware geymir tölvukerfi eða gögnin sem það inniheldur í gíslingu þar til greitt er.

• Scareware er tegund spilliforrita sem byggir á því að sannfæra notandann um að grípa til sérstakra aðgerða út frá ótta.

• Rootkit er spilliforrit sem er hannað til að breyta stýrikerfinu til að búa til bakdyr.

• Veira er illgjarn keyra legur kóði sem er festur við aðra keyra lega skrár.

• Tróverskur hestur er spilliforrit sem framkvæmir skaðlegar aðgerðir í skjóli æskilegrar aðgerðar.

• Ormar eru illgjarn kóði sem endurtaka sig með því að nýta sér varnarleysi sjálfstætt í netkerfum.

• MitM gerir árásarmanninum kleift að taka stjórn á tæki án vitundar notandans.

1. Það hafi verið breitt skránna, tölvan hægir og háa aukning í CPU notkun.

• Árásarmaðurinn hagar manni sem þekkir lykilorðið til að gefa það upp.

• Árásarmaðurinn reynir nokkur möguleg lykilorð til að giska á lykilorðið.

1. Dæmi um vefveiðar er tölvupóstur sem er fals til að líta út eins og hann hafi verið sendur af smásöluverslun þar sem notandinn er beðinn um að smella á krækju til að fá verðlaun.

Skref 1. Safnaðu upplýsingum um markkerfið.

Skref 2. Eitt stykki af viðeigandi upplýsingum sem lært var í skrefi 1.

Skref 3. Þegar stýrikerfi og útgáfa miðans er þekkt leitar árásarmaðurinn að þekktum veikleikum sem eru sértækir fyrir þá útgáfu af stýrikerfi eða annarri stýrikerfisþjónustu.

Skref 4. Þegar varnarleysi er fundið leitar árásarmaðurinn að áður skrifaðri nýtingu til að nota.

1. Með DoS árás, þegar netkerfi, gestgjafi eða forrit er sent gífurlegt magn gagna á hraða sem það ræður ekki við. Þetta veldur því að hægja á flutningi eða svörun eða hrun á tæki eða þjónustu. En með DDoS árás byggir árásarmaður net sýktra gestgjafa, sem kallast botnet. Hinir sýktu gestgjafar eru kallaðir uppvakningar.

stjórnað af stjórnkerfum.

1. Notaðu margar aðferðir til að skerða markmið.
2. Með langt og flókið lykilorð, notaðu áreiðanlegt antimalware forrit og slökkva á Bluetooth ef þú þarft ekki að nota það.
3. Nota setninga sem staðin fyrir eitt orð, breytta nokkra bókstafa í tölustaff.
4. Atriðunum gæti verið eytt óviljandi eða í beinni skemmdarverkum.
5. Að þurfa nota síman til að loga inn.
6. Það er opinn staðlaða siðareglur sem leyfa skilríkjum endanotanda að fá aðgang að forritum þriðja aðila án þess að afhjúpa lykilorð notanda.
7. Notaðu það bara ef þú vilt ekki að fjölskyldan skoði sögu vafrans þíns.
8. Það verður slæmt fyrir viðskipti.
9. „Kill Chain“ er stigi í árásar upplýsingakerfa.  
   malware fer á mismunandi stigum, skref fyrir skref eins og þetta: Könnun> Vopnun> Afhending> Nýting> Uppsetning> Skipun og stjórn> Aðgerð.