Nafn: _____ Dagsetning: _____ Stig: _____

Gíslatökuárásir og fyrirtæki Endurheimt

Framkvæmd farms, dulkóðun skráa, afrit utan nets, innilokunarferli og hamfaraendurheimt.

NÁMSYFIRLIT UM GÍSLATÖKUÁRÁSIR

VARIÐ
GAGNADULKÓÐUN
256-bita AES staðall

UPPFYLLIR KRÖFUR
ALÞJÓÐLEGIR STAÐLAR
Rammar GDPR og CCPA

ZERO-TRUST
AÐGANGSSTEFNA
Fjölþátta auðkenning

Velkomin! Þetta verkefnahefti leiðir þig í gegnum gíslatökuárásir og endurheimt fyrirtækja. Þú munt kynnast keyrslu skaðlegrar hleðslu, skráadulkóðun, afritum utan nets, innilokun ógna, rafmyntagreiðslum og neyðarendurheimtaráætlunum.

ÁFANGAR VERKEFNABLAÐSINS

- [ ] **Hluti 1-4: Náðu tökum á netöryggi og varnir gegn ógnum.**
- [ ] **Hluti 5-7: Leystu krossgátur og orðaleitarþrautir.**
- [ ] **Hluti 8-9: Leystu dæmisögur og dulmálsáskorun.**
- [ ] **Hluti 10: Farðu yfir síður með algengum spurningum, grunnstig og framhaldsstig.**
- [ ] **Hluti 11: Kannaðu 10 áhugaverðar staðreyndir úr raunheimum.**
- [ ] **Auka: áskorunin Hugsaðu hratt.**

Opnaðu netöryggisleiðarvísi VPN.com

URL: https://www.vpn.com/is/netoryggd/lausnargjaldshugbundararas/

Námsvegvísir þinn: endurheimt eftir gíslatökuforrit

- Gerðu greinarmun á Trójuhesti, gíslatökuhugbúnaði og njósnahugbúnaði.
- Greindu skaðlegar skrár í öruggu sandkassaumhverfi.
- Mótaðu verklag til að einangra net og halda broti í skefjum.

LEIÐBEININGAR UM GÍSLATÖKUÁRÁSIR

Svaraðu fjölvalsspurningunum og satt/ósatt-spurningunum, kláraðu eyðufyllingarsetningarnar með orðabankanum, paraðu saman skilgreiningar og leystu krossgátuna og orðaleitina. Nýttu þekkingu þína á endurheimt eftir gagnagíslatöku. Ljúktu með aukaverkefninu Hugsaðu hratt.

GÍSLATÖKUÁRÁSIR OG ENDURHEIMT EFTIR ÁFÖLL (INNGANGUR)

Skaðlegur hleðslukóði gíslatökuforrita læsir geymslu kerfisins með dulritun og krefst greiðslu í rafmynt fyrir afkóðunarlykla. Til að draga úr þessari ógn þarf reglur um netaðskilnað, greiningu spilliforrita í sandkassa og traust köld afrit án nettengingar.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.

Áfangi 1: Fjölvalsáskorun

1 **1. Hver er meginleið kúgunarhugbúnaðarárásar?**

- A. Dulkóðun notendaskráa til að neita aðgangi að kerfinu
- B. Að sprauta skaðlegum SQL-skipunum í innsláttarreiti
- C. Að hlera netpakka á opinberu Wi-Fi-neti
- D. Að falsa tölvupósthausa til að sniðganga SPF-staðfestingu

2 **2. Hvað er ótengt (kalt) afrit?**

- A. Geymsluafrit sem er aftengt netinu til að verja það gegn útbreiðslu spilliforrita
- B. Afrit sem er geymt á harða diski aðalvefþjónsins
- C. Tímabundið skyndiminni skráningarskráa kerfisins
- D. Stjórnunartól til að endurstilla lykilorð notenda

3 **3. Hvernig ættu öryggisteymi að einangra sýkt kerfi í gíslatökuárás?**

- A. Aftengja netsnúrur og slökkva strax á þráðlausum viðmótum
- B. Uppfæra gagnagrunn vírusvarnarundirskrifta
- C. Slökktu á aðal-DNS-netþjóninum
- D. Endurnefna sýktar skráarendingar

4 **4. Hvers vegna ráðleggja öryggisstofnanir gegn því að greiða lausnargjald kúgunarhugbúnaðar?**

- A. Greiðsla hvetur árásaraðila og tryggir ekki afhendingu afkóðunarlykils
- B. Það ógildir sjálfkrafa allar tryggingar fyrirtækisins
- C. Það lætur alla viðskiptavini vita sjálfkrafa með tölvupósti
- D. Það skemmir eftirstandandi afritunarskrár kerfisins

5 **5. Hvað er áætlun um endurheimt eftir áföll (DRP)?**

- A. Skipulagt ferli til að endurheimta rekstur og gögn eftir að kerfi hefur verið brotist inn í
- B. Eldveggsstilling sem kortleggir innkomnar netgáttir
- C. Gagnagrunnsskema sem telur upp stjórnandaréttindi notenda
- D. Auðkenningarsamskiptaregla fyrir tölvupóst sem hafnar fölsuðum lénum

Áfangi 2: Satt eða ósatt

6 Spurning 6

6. Skaðlegur hleðslukóði gíslatökuforrita getur auðveldlega dreifst til afrita á netinu sem tengd eru við netið.

Satt Ósatt

7 Spurning 7

7. Að greiða rafmyntalausnargjaldið tryggir að skrár verði afkóðaðar með góðum árangri.

Satt Ósatt

8 Spurning 8

8. Að aftengja sýkt kerfi frá netinu hjálpar til við að stöðva útbreiðslu kúgunarhugbúnaðar til nálægra kerfa.

Satt Ósatt

9 Spurning 9

9. Samhverf dulritun er aldrei notuð af gíslatökuforritum til að dulkóða geymslu kerfa.

Satt Ósatt

10 Spurning 10

10. Regluleg prófun á endurheimtarferlum gagna er mikilvægur hluti hamfarabata.

Satt Ósatt

Áfangi 3: Lykilhugtök fyllt inn

Lestu hverja setningu hér að neðan og fylltu í eyðuna með réttu hugtaki úr orðabankanum.

1. Til að loka á aðgang að staðbundnum skrám er beitt dulmálslegri _____ .
2. Virki skaðlegi kóðinn sem keyrður er á kerfi er _____ .
3. Aftengd afrit á geymslu utan starfsstöðvar eru öruggt _____ .
4. Til að stöðva útbreiðslu spilliforrits þarf _____ endapunkta á neti.
5. Greiðslan í rafmynt sem netglæpamenn krefjast er _____ .
6. Að koma rekstrargagnaskrám aftur í lag eftir hamfarir kallast _____ .

ORÐABANKI

DULKÓÐUN EINANGRUN ENDURHEIMT FARMUR HAMFARIR KALT AFRIT LAUSNARGJALD TRÓJUHESTUR

Skrifaðu svörin þín hér:

1.
2.
3.
4.
5.
6.

Áfangi 4: Pörun hugtaka um öryggi

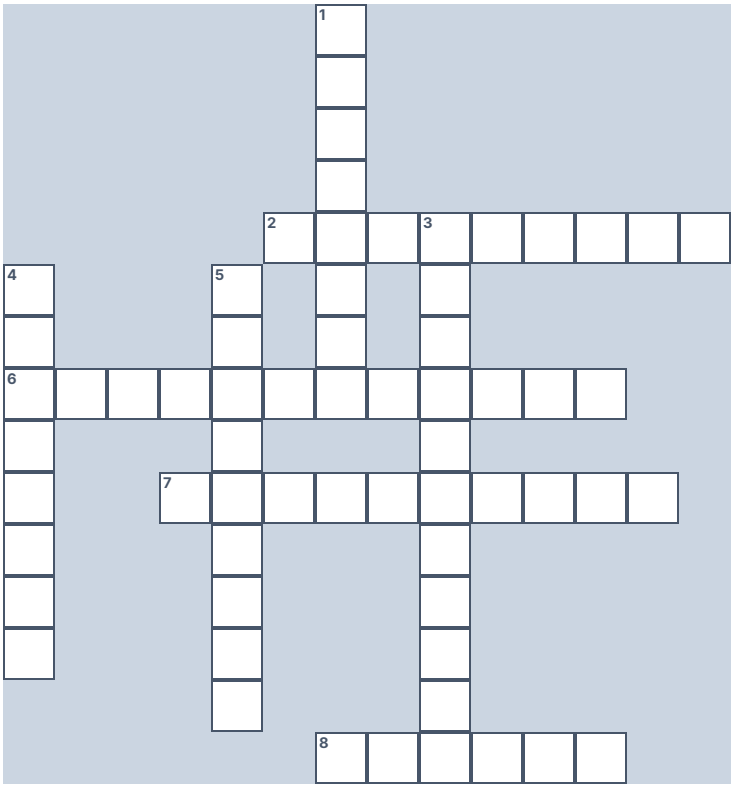
PÖRUN SKILGREININGA

Paraðu hvert hugtak til vinstri við rétta skilgreiningu til hægri með því að skrifa samsvarandi bókstaf (A-H) í útfyllanlega reitinn.

☐	1. DULKÓÐUN	A	Að aftengja sýkt netkerfi.
☐	2. FARMUR	B	Skaðleg skrá dulbúin sem hrein.
☐	3. AFRIT Í KALDGEYMSLU	C	Að læsa skrám með dulritun.
☐	4. EINANGRUN	D	Alvarleg röskun á kerfi.
☐	5. LAUSNARGJALD	E	Keyrsla á skaðlegum hugbúnaði.
☐	6. ENDURHEIMT	F	Aftengt afrit án nettengingar.
☐	7. HAMFARIR	G	Endurheimta gagnagrunn úr afriti.
☐	8. TRÓJUHESTUR	H	Beiðni um útgreiðslu dulritunarlykils.

Áfangi 5: Krossgáta

Leystu krossgátuna með því að slá stafi inn í virku hvítu reitina. Tölurnar vísa til vísbendinganna hér að neðan.



LÁRÉTT

2. Aftengt afrit utan nets (9)

6. Krafa um greiðslu fyrir dulmálslykil (12)

7. Endurheimt gagnagrunns úr afriti (10)

8. Virkur skaðlegur hugbúnaður keyrður (6)

LÓÐRÉTT

1. Atvik með mikilli röskun á kerfum (8)

3. Skaðleg skrá sem dulbýr sig sem meinlaus (11)

4. Læsing skráa með dulmáli (8)

5. Aftenging sýktra netkerfa (9)

Áfangi 5, valkostur: Aðgengilegar vísbendingar fyrir krossgátu

Notendur skjálesara og lyklaborðs geta slegið svör krossgátunnar beint inn í textareitina hér að neðan.

LÁRÉTT

2 lárétt: Aftengt afrit utan nets (9 stafir):

6 lárétt: Krafa um greiðslu fyrir dulmálslykil (12 stafir):

7 lárétt: Endurheimt gagnagrunns úr afriti (10 stafir):

8 lárétt: Virkur skaðlegur hugbúnaður keyrður (6 stafir):

LÓÐRÉTT

1 lóðrétt: Atvik með mikilli röskun á kerfum (8 stafir):

3 lóðrétt: Skaðleg skrá sem dulbýr sig sem meinlaus (11 stafir):

4 lóðrétt: Læsing skráa með dulmáli (8 stafir):

5 lóðrétt: Aftenging sýktra netkerfa (9 stafir):

Áfangi 6: Falið orð í orðaleit

Finndu 8 lykilhugtök sem eru falin í reitnum hér að neðan. Orð geta verið lárétt, lóðrétt eða á ská.

I Đ S R M E I K T Ö U É R X É
R N A A R Ó N A P Ú E Þ R J S
U U Ú T D N Æ L B F I T Ý Y Í
T Đ A S F Ö Æ T Æ K N F I M S
S Ó J L A L U A Ó G A P R E G
E K Ö A R O X F F V N B Æ N T
H L Æ Á M G L R Ö G G J O D P
U U N Ý U B L I Ö Æ R F Þ U Ó
J D Y V R K V T P Á U O X R Ú
Ó L G X D Þ V J S Á N Ý Ö H Þ
R L A U S N A R G J A L D E M
T T R Ý I Ó Đ A D J R Y Ý I Ý
K Í H A M F A R I R H Ú H M F
Á É I K U T Y S Ö E H É T T D
A L P B Ö M J X S V A T Ý J M

ORÐALISTI

DULKÓÐUN, FARMUR, KALTAFRIT, EINANGRUN, LAUSNARGJALD, ENDURHEIMT, HAMFARIR, TRÓJUHESTUR

Áfangi 6, valkostur: Aðgengileg orðaforðapörun

Paraðu hvert af hugtökunum 8 úr orðaleitinni við rétta skilgreiningu með því að skrifa bókstafinn (A-H) í eyðuna.

HUGTÖK
A. DULKÓÐUN
B. FARMUR
C. KALTAFRIT
D. EINANGRUN
E. LAUSNARGJALD
F. ENDURHEIMT
G. HAMFARIR
H. TRÓJUHESTUR

SKILGREININGAR OG PÖRUNARREITIR

1. Aftengt afrit utan nets. ____
2. Skaðleg skrá sem dulbýr sig sem meinlaus. ____
3. Læsing skráa með dulmáli. ____
4. Krafa um greiðslu fyrir dulmálslykil. ____
5. Aftenging sýktra netkerfa. ____
6. Atvik með mikilli röskun á kerfum. ____
7. Virkur skaðlegur hugbúnaður keyrður. ____
8. Endurheimt gagnagrunns úr afriti. ____

Áfangi 7: Áskorun með ruglaðum orðum

Raðaðu stöfunum hér að neðan í rétta röð til að afhjúpa lykilhugtök um netöryggi. Skrifaðu svörin þín í reitina sem fylgja.

1. **UKÓDÐUNL** _____

2. **TKITAFRAL** _____

3. **LAGRLJUADNAS** _____

4. **FIRRAHAM** _____

5. **MRRFUA** _____

6. **UAIRGENNN** _____

7. **NUEEHIMTRD** _____

8. **TERHÓTURUSJ** _____

Aukaverkefni: Hugsaðu hratt

3 SVÖR Í HVERJUM FLOKKI. SÁ VINNUR SEM FYLLIR FYRST ÚT LISTANN.

1	Upplýsingar sem þú ættir aldrei að deila			
2	Tæki sem hægt er að brjótast inn í			
3	Ástæður fyrir því að greiða ekki lausnargjald			
4	Öruggar venjur sem þú getur byrjað á í dag			
5	Öryggisverkfæri sem þú þekkir			
6	Leiðir til að vernda reikningana þína			
7	Merki þess að tölva sé sýkt			
8	Staðir til að geyma afrit			
9	Skrár sem þú vilt aldrei missa			
10	Leiðir sem kúgunarhugbúnaður dreifist			
11	Hlutir til að gera á fyrstu klukkustund árásar			
12	Fólk sem hafa skal samband við í árás			
13	Hlutir sem kúgunarhugbúnaður getur læst			
14	Orð tengd netöryggi			
15	Stofnanir sem oft verða fyrir árásum			

Áfangi 8: Dæmisögur um netöryggi

Nýttu hugtökin sem þú hefur lært til að leysa raunveruleg dæmi hér að neðan.

DÆMISAGA 1: AFMÖRKUN LAUSNARHUGBÚNAÐAR Í FYRIRTÆKI

👨‍💻

Aðstæður: Brotist hefur verið inn á staðarnet fyrirtækis með virku gíslatökuforriti. Lykilskráarnetþjónar eru farnir að sýna skráarendingar með .locked.

Umræðuspurning: Lýstu skrefum til að hefta útbreiðslu og gerðu grein fyrir gagnaendurheimtarferlinu.

DÆMISAGA 2: MAT Á AFRITUNARARKITEKTÚR UTAN NETS

👨‍💻

Aðstæður: Stórfyrirtæki vill hanna gagnaafritunarstefnu sem dregur úr hættu á að afritum sé ógnað, jafnvel þótt aðalstaðarnetið sé algjörlega yfirtekið af kúgunarhugbúnaði.

Umræðuspurning: Hannaðu öruggt geymsluhvelfingarkerfi fyrir afrit án nettengingar.

Áfangi 9: Leystu dulmálið

Netöryggissérfræðingur ver netkerfiseignir gegn ógnaraðilum á netinu. Notaðu lykilinn „bókstafur í tölu“ hér að neðan til að afkóða skilaboðin með því að skrifa samsvarandi bókstafi í auðu reitina.

DULMÁLSLYKILL: STAFIR Í TÖLUR

A=1 Á=2 B=3 C=4 D=5 Đ=6 E=7 É=8 F=9 G=10 H=11 I=12

Í=13 J=14 K=15 L=16 M=17 N=18 O=19 Ó=20 P=21 Q=22 R=23 S=24

T=25 U=26 Ú=27 V=28 W=29 X=30 Y=31 Ý=32 Z=33 Þ=34 Æ=35 Ö=36

7	18	5	26	23	11	7	12	17	25	26		5	26	16	15	20	6	26	6

10	36	10	18		27	23		15	36	16	5	26		1	9	23	12	25	12

Afkóðuð skilaboð:

ÁBENDING: HVER TALA STENDUR FYRIR STÖÐU STAFSINS Í STAFRÓFINU (T.D. 1 = A, 2 = B, 36 = Ö).

Áfangi 10: Algengar spurningar um netöryggi – grunnstig (Hluti A)

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q1: Hvað er gíslatökuhugbúnaður?

Gíslatökuforrit er skaðlegur hugbúnaður sem er hannaður til að loka á aðgang að tölvukerfum eða skrám þar til lausnargjald er greitt.

Q2: Hvernig dreifist gíslatökuhugbúnaður?

Með viðhengjum í vefveiðapósti, óuppfærðum veikleikum í hugbúnaði og sýktum fjaraðgangskerfum. [1]

Q3: Hvers vegna er beðið um greiðslu í rafmynt?

Rafmyntir eins og Bitcoin bjóða upp á hlutfallslega nafnleynd, sem gerir löggæslu erfitt fyrir að rekja fé.

Q4: Lokar vírusvörn á gíslatökuforrit?

Já, en vírusvörn byggð á undirskriftum getur brugðist gegn nýsmíðuðum zero-day hleðslum kúgunarhugbúnaðar.

Q5: Hvað er afrit án nettengingar (air-gapped backup)?

Afritunareintak sem hefur engin líkamleg eða rökræn tengsl við aðalnetið og er því varið gegn útbreiðslu.

Áfangi 10: Algengar spurningar um netöryggi – grunnstig (Hluti B)

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q6: Hvað er tvöföld fjárkúgun (double extortion)?

Þegar árásaraðilar dulkóða ekki aðeins skrár heldur stela einnig viðkvæmum gögnum til að hóta opinberum leka ef ekki er greitt.

Q7: Hvað er afkóðunarforrit (decryptor)?

Hugbúnaðartól sem inniheldur dulritunarlykilinn sem þarf til að endurheimta læstar skrár í lesanlegan texta.

Q8: Hvernig greinir þú gíslatökuforrit snemma?

Með því að vakta skráakerfi eftir skyndilegum, miklum skráabreytingum og endurnefningum.

Q9: Hvaða hlutverki gegna tryggingar?

Netöryggistrygging getur hjálpað til við að standa straum af endurheimtarkostnaði, en tryggingaskilmálar og reglur um greiðslu lausnargjalds eru mismunandi eftir skilmálum.

Q10: Ætti ég að endurræsa sýkt kerfi?

Nei, endurræsing getur eytt sönnunargögnum í rokgjörnu minni; einangraðu tækið frá netinu í staðinn. [1]

Áfangi 10: Algengar spurningar um öryggi – framhaldsstig (Hluti C)

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q1: Hvernig notar gíslatökuhugbúnaður ósamhverfa dulkóðun?

Það notar opinberan lykil sem er innbyggður í spilliforritið til að dulkóða skrár og krefst einkalykils árásaraðilans til að afkóða þær.

Q2: Hvers vegna er samhverf dulkóðun einnig notuð?

Samhverf dulkóðun (eins og AES) er hröð og getur læst risastórum gagnagrunnum á nokkrum mínútum, á meðan ósamhverfir lyklar verja AES-lykilinn.

Q3: Hvað er rökræn skipting (logical segmentation)?

Að skipta netum í einangruð svæði, sem kemur í veg fyrir að spilliforrit berist til hliðar frá vinnustöðvum yfir á kjarnaþjóna.

Q4: Hvað er WORM-geymsla?

Write-Once, Read-Many miðlar, sem koma í veg fyrir að afritagögnum sé breytt, þau yfirskrifuð eða þeim eytt af hleðslum kúgunarhugbúnaðar.

Q5: Hvað eru skuggaafrit (shadow copies)?

Staðbundin öryggisafrit sem Windows býr til; gíslatökuforrit eyða þeim yfirleitt fyrst með stjórnendaverkfærum.

Áfangi 10: Algengar spurningar um öryggi – framhaldsstig (Hluti D)

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q6: Hvernig gerir þjófnaður á innskráningarupplýsingum gíslatökuforrit mögulegt?

Árásarmenn kaupa lekin stjórnandainnskráningarupplýsingar til að skrá sig inn um fjarskjáborð og keyra gagnagíslatökuforrit handvirkt um allt netið.

Q7: Hvað er prófun á endurheimt með æfingakeyrslu (dry-run)?

Að endurheimta afritaða gagnagrunna reglulega í einangruð prófunarumhverfi til að staðfesta að endurheimtarhraði og gagnaheilleiki uppfylli viðmið fyrir hamfarabata.

Q8: Hvernig stöðvar greining og viðbrögð á endabúnaði (EDR) gíslatökuforrit?

Með því að greina hegðun ferla (t.d. hraða dulkóðun) og stöðva grunsamlega forritið hratt.

Q9: Hvað er gíslatökuforrit sem þjónusta (ransomware-as-a-service, RaaS)?

Sérleyfislíkan þar sem höfundar spilliforrita leigja samstarfsaðilum smíðatól fyrir kúgunarhugbúnað gegn hlutfalli af greiðslum.

Q10: Hvernig kveikir óplástrað RDP á gíslatökuhugbúnaði?

Berskjölduð, ólöguð Remote Desktop Protocol-gátt gerir árásaraðilum kleift að ráðast á innskráningar með þrotlausum prófunum og ræsa spilliforrit handvirkt.

Hluti 11: 10 staðreyndir um netöryggi og innsýn úr raunheimum

Farðu yfir raunverulegar staðreyndir um öryggisbrot, varnarkerfi og reglufylgnistaðla.

1. INNSÝN Í ÖRYGGI

Gíslatökuaðilar nota oft verkfæri eins og vssadmin.exe til að eyða skuggaafritum í Windows og loka á staðbundna endurheimt. [1]

2. INNSÝN Í ÖRYGGI

Samhverfir AES-256 lyklar eru yfirleitt notaðir til að dulkóða skráargögn, sem síðan eru læst með opinberum RSA-lyklum.

3. INNSÝN Í ÖRYGGI

Það getur tekið vikur að jafna sig eftir vel heppnaða gagnagíslatöku, og þess vegna skipta prófuð ótengd afrit máli.

4. INNSÝN Í ÖRYGGI

FBI styður ekki greiðslu lausnargjalds og varar við því að greiðsla tryggi ekki að þú fáir gögnin þín aftur. [2]

5. INNSÝN Í ÖRYGGI

Neyðaráætlanir um endurheimt (DRP) ættu að skilgreina markmið um endurheimtartíma (RTO) og markmið um endurheimtarpunkt (RPO).

6. INNSÝN Í ÖRYGGI

FBI mælir með afritum sem eru dulkóðuð og óbreytanleg, sem þýðir að ekki er hægt að breyta þeim eða eyða. [3]

7. ÖRYGGISINNSÝN

Höfundar gíslatökuforrita nota háþróaða dulbúningartækni til að komast framhjá hefðbundnum undirskriftarbyggðum vírusskönnum.

8. ÖRYGGISINNSÝN

Netskipting takmarkar hliðarhreyfingu og hjálpar til við að stöðva útbreiðslu gíslatökuforrita út fyrir fyrstu sýktu vélina. [3]

9. ÖRYGGISINNSÝN

Berskjölduð, illa varin fjarþjónusta eins og Remote Desktop Protocol (RDP) er algeng aðkomuleið gíslatökuhugbúnaðar. [1]

10. INNSÝN Í ÖRYGGI

CISA ráðleggur að geyma dulkóðuð afrit utan nets, þar sem mörg afbrigði lausnarhugbúnaðar leita uppi og eyða afritum sem hægt er að ná til. [1]

Tæknilegar heimildir og tilvísanir

Námsleiðbeiningarnar og gagnvirku þrautirnar eru unnar úr alþjóðlegum stöðlum NIST og OWASP og kröfum um persónuverndarsamræmi.

FRÆÐILEGAR HEIMILDIR OG HEIMILDIR ÚR ATVINNUGREININNI

[1] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.

https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Lausnir: Áfangi 1 – Fjölval

1 **Spurning 1** **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hver er meginleið kúgunarhugbúnaðarárásar? → Dulkóðun notendaskráa til að neita aðgangi að kerfinu

2 **Spurning 2** **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað er ótengt (kalt) afrit? → Geymsluafrit sem er aftengt netinu til að verja það gegn útbreiðslu spilliforrita

3 **Spurning 3** **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvernig ættu öryggisteymi að einangra sýkt kerfi í gíslatökuárás? → Aftengja netsnúrur og slökkva strax á þráðlausum viðmótum

4 **Spurning 4** **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvers vegna ráðleggja öryggisstofnanir gegn því að greiða lausnargjald kúgunarhugbúnaðar? → Greiðsla hvetur árásaraðila og tryggir ekki afhendingu afkóðunarlykils

5 **Spurning 5** **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað er áætlun um endurheimt eftir áföll (DRP)? → Skipulagt ferli til að endurheimta rekstur og gögn eftir að kerfi hefur verið brotist inn í

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Spurning 6** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Skaðlegur hleðslukóði gíslatökuforrita getur auðveldlega dreifst til afrita á netinu sem tengd eru við netið.

7 **Spurning 7** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: FBI varar við því að greiðsla tryggir ekki að þú fáir nokkur gögn til baka.

8 **Spurning 8** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Satt: CISA ráðleggur að taka sýkta hýsla úr sambandi eða taka netið af línunni til að hefta útbreiðslu.

9 **Spurning 9** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: kúgunarhugbúnaður dulkóðar yfirleitt skrár með hröðum samhverfum dulmálum á borð við AES.

10 **Spurning 10** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Regluleg prófun á endurheimtarferlum gagna er mikilvægur hluti hamfarabata.

Orðalyklar og matskvarði

Einkunnaviðmið kennara: Gefðu 1 stig fyrir hverja rétta pörun (alls 8 stig) og hvert samhengishugtak (alls 6 stig).

ÁFANGI 4: LAUSNIR – PÖRUN HUGTAKA

C 1. DULKÓÐUN	E 2. FARMUR	F 3. AFRIT Í KALDGEYMSLU	A 4. EINANGRUN
H 5. LAUSNARGJALD	G 6. ENDURHEIMT	D 7. HAMFARIR	B 8. TRÓJUHESTUR

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

1 DULKÓÐUN	2 FARMUR	3 KALT AFRIT	4 EINANGRUN
5 LAUSNARGJALD	6 ENDURHEIMT		

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

1 C – KALTAFRIT	2 H – TRÓJUHESTUR	3 A – DULKÓÐUN	4 E – LAUSNARGJALD
5 D – EINANGRUN	6 G – HAMFARIR	7 B – FARMUR	8 F – ENDURHEIMT

UMRÆÐUATRIÐI FYRIR KENNARA

Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt DULKÓÐUN, FARMUR og AFRIT Í KALDGEYMSLU með eigin orðum og gefið dæmi um hvert hugtak.

Dæmisögur:
Biddu nemendur að styðja tillögur sínar með staðreyndum úr verkefnablaðinu en ekki ágiskunum.

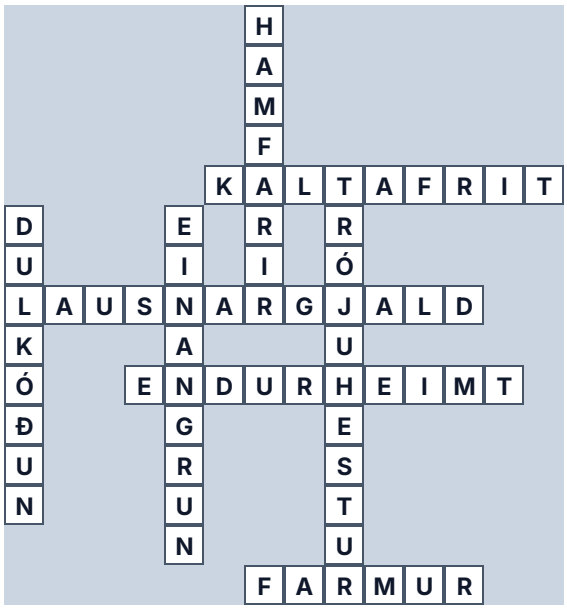
Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR

I	Đ	S	R	M	E	I	K	T	Ö	U	É	R	X	É
R	N	A	A	R	Ó	N	A	P	Ú	E	Þ	R	J	S
U	U	Ú	T	D	N	Æ	L	B	F	I	T	Ý	Y	Í
T	Đ	A	S	F	Ö	Æ	T	Æ	K	N	F	I	M	S
S	Ó	J	L	A	L	U	A	Ó	G	A	P	R	E	G
E	K	Ö	A	R	O	X	F	F	V	N	B	Æ	N	T
H	L	Æ	Á	M	G	L	R	Ö	G	G	J	O	D	P
U	U	N	Ý	U	B	L	I	Ö	Æ	R	F	Þ	U	Ó
J	D	Y	V	R	K	V	T	P	Á	U	O	X	R	Ú
Ó	L	G	X	D	Þ	V	J	S	Á	N	Ý	Ö	H	Þ
R	L	A	U	S	N	A	R	G	J	A	L	D	E	M
T	T	R	Ý	I	Ó	Đ	A	D	J	R	Y	Ý	I	Ý
K	Í	H	A	M	F	A	R	I	R	H	Ú	H	M	F
Á	É	I	K	U	T	Y	S	Ö	E	H	É	T	T	D
A	L	P	B	Ö	M	J	X	S	V	A	T	Ý	J	M

LAUSN KROSSGÁTUNNAR



LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

LÁRÉTT

2 lárétt: KALTAFRIT Aftengt afrit utan nets (9 stafir)

6 lárétt: LAUSNARGJALD Krafa um greiðslu fyrir dulmálslykil (12 stafir)

7 lárétt: ENDURHEIMT Endurheimt gagnagrunns úr afriti (10 stafir)

8 lárétt: FARMUR Virkur skaðlegur hugbúnaður keyrður (6 stafir)

LÓÐRÉTT

1 lóðrétt: HAMFARIR Atvik með mikilli röskun á kerfum (8 stafir)

3 lóðrétt: TRÓJUHESTUR Skaðleg skrá sem dulbýr sig sem meinlaus (11 stafir)

4 lóðrétt: DULKÓÐUN Læsing skráa með dulmáli (8 stafir)

5 lóðrétt: EINANGRUN Aftenging sýktra netkerfa (9 stafir)

Lausnir: Stafaruglingur og dulmál

Lausnalykill fyrir virkni um að raða orðaforða og Secret Cipher Challenge.

LYKILL ORÐARAÐAR

1. U K Ó D Đ U N L — **DULKÓÐUN**
2. T K I T A F R A L — **KALTAFRIT**
3. L A G R L J U A D N A S — **LAUSNARGJALD**
4. F I R R A H A M — **HAMFARIR**
5. M R R F U A — **FARMUR**
6. U A I R G E N N N — **EINANGRUN**
7. N U E E H I M T R D — **ENDURHEIMT**
8. T E R H Ó T U R U S J — **TRÓJUHESTUR**

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"ENDURHEIMTU DULKÓÐUÐ GÖGN ÚR KÖLDU AFRITI"

Lausnir dæmisagna

A Dæmisaga 1: Afmörkun lausnarhugbúnaðar í fyrirtæki

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Staðarnet fyrirtækis hefur verið brotist inn á með virkri gagnagíslatöku. Lykilskráaþjónar eru farnir að sýna skráarendingar með .locked.
- Ráðlögð aðferð og lausn: Aftengdu alla netþjóna sem verða fyrir áhrifum frá staðarnetinu. Bindaðu enda á virkar stjórnendalotur. Endurheimtu óskemmdar skrár úr öruggu afritunarkerfi án nettengingar sem er skrifvarið.

B Dæmisaga 2: Mat á afritunararkitektúr utan nets

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Aðstæður til greiningar: Fyrirtæki vill hanna afritunarstefnu sem dregur úr hættunni á að afrit séu í hættu, jafnvel þótt gíslatökuforrit nái algjörri stjórn á staðarnetinu.
- Ráðlögð aðferð og lausn: Innleiddu write-once-read-many (WORM) geymslu. Komdu á rökrænni loftrauf með því að aftengja afritunarkerfið frá öllum netum og framfylgdu daglegum skiptum á geymslumiðlum.