Nafn: _____ Dagsetning: _____ Stig: _____

Grunnatriði netöryggis og ógnir á netinu Forvarnir

Netöryggisógnir, netveggir, fjölþátta auðkenning, öryggisrammar

NÁMSYFIRLIT: GRUNNATRIÐI NETÖRYGGIS

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 grunnatriði netöryggis og varna gegn ógnum á netinu. Þú munt kynnast ógnum af völdum spilliforrita, fjölþátta auðkenningu, neteldveggjum og viðbragðsramma við atvikum.

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/

Námsvegvísir þinn: grunnatriði netöryggis

- Greindu algengar leiðir spilliforrita, vefveiða og innbrota í net fyrirtækja.
- Innleiddu hefðbundnar netöryggisstýringar, þar á meðal MFA, eldveggi og vörn endabúnaðar.
- Metðu viðbragðsferla við atvikum til að draga úr áhrifum gagnaleka.
- Greindu áhættuþætti stofnana og öryggissamræmingu samkvæmt leiðbeiningum NIST.
- Stilltu öryggisvenjur til að draga úr sjálfvirkri innskráningarfyllingu.

LEIÐBEININGAR UM NETÖRYGGI

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

GRUNNATRIÐI NETÖRYGGIS OG FORVÖRN GEGN ÓGNUM (INNGANGUR)

Netöryggi ver net, kerfi og gögn gegn óleyfilegum stafrænum árásum. Að þróa traustar öryggisvenjur, stilla eldveggi, krefjast fjölþátta auðkenningar og þjálfa starfsfólk í að þekkja ógnir eru lykilþættir í netvörnum fyrirtækja.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.

Áfangi 1: Fjölvalsáskorun

1 **1. Hvert er meginmarkmið vefveiðaárásar?**

- A. Að stela auðkennum og viðkvæmum notendagögnum
- B. Að bæta sýnileika vefsvæðis í leitarvélum
- C. Að auka bandbreidd netsins
- D. Umsjón með afritun á varagagnaveri

2 **2. Hvaða búnaður veitir öflugustu reikningsvörnina?**

- A. Fjölþátta auðkenning með vélbúnaðarlyklum
- B. Flókin lykilorð sem eru uppfærð á þrjátíu daga fresti
- C. Að takmarka innskráningu á reikninga við vinnutíma
- D. Að fela notandanafn reiknings fyrir opinberum skrám

3 **3. Hvað einkennir hleðslu í kúgunarhugbúnaðarsýkingu?**

- A. Að dulkóða kerfisskrár og krefjast greiðslu
- B. Að skrá lyklaborðsslátt hljóðlaust á fjarnetþjóna
- C. Að koma óleyfilegum auglýsingum fyrir í vöfrum
- D. Að nota örgjörvaafl tölvunnar til að grafa eftir rafmynt

4 **4. Hvernig hefur núlldagsveila áhrif á öryggisvarnir?**

- A. Það beinist að óbættum, óþekktum veikleikum
- B. Það slekkur sjálfkrafa á eldvegg fyrirtækisins
- C. Það þvingar kerfið til að endurræsa sig með valdi
- D. Það kostar ekkert að bregðast við

5 **5. Hvaða rammi stýrir öryggiseftirliti fyrirtækja?**

- A. Leiðbeiningar NIST Cybersecurity Framework
- B. W3C HTML5 skjalaskemalýsingar
- C. Uppsetningarhandbækur fyrir prentarareklara
- D. Skilgreiningar IETF á leiðarvalssamskiptareglum

Áfangi 2: Satt eða ósatt

6 Spurning tf 6

6. Vefveiðaárásir beinast aðeins að einkapóstföngum.

○ Satt ○ Ósatt

7 Spurning tf 7

7. Fjölþátta auðkenning hjálpar til við að loka fyrir lykilorðafyllingarárásir (credential stuffing).

○ Satt ○ Ósatt

8 Spurning tf 8

8. Eldveggir skoða netumferð til að loka á óheimilan aðgang um netgáttir.

○ Satt ○ Ósatt

9 Spurning tf 9

9. Úrbætur vegna núlldagaárása krefjast venjulegra uppfærslna á vírusvarnarskilgreiningum.

○ Satt ○ Ósatt

10 Spurning tf 10

10. Hunangsgildra (honeypot) er tálbeitunetþjónn sem notaður er til að lokka netglæpamenn.

○ Satt ○ Ósatt

Áfangi 3: Lykilhugtök fyllt inn

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

1. Netstjórar setja upp netvörn sem kallast _____ til að sía komandi umferð.

2. Árásaraðili notar svokallaða _____ til að komast framhjá öryggisuppfærslum kerfisins.

3. Árásaraðilar senda falsaðan tölvupóst til að standa fyrir herferðum sem kallast _____ gegn starfsmönnum.

4. Gíslaforrit er skaðleg gerð hugbúnaðar sem kallast _____ og læsir gögnum notenda.

5. Öflugt _____ lykilorða dregur úr hættu á þjófnaði á auðkennum.

6. Til að vernda viðkvæm samskipti nota notendur samskiptareglur sem byggja á _____ .

ORÐABANKI

DULKÓÐUN ELDVEGGUR FJÖLÞÁTTA GÍSLAFORRIT HREINLÆTI NÚLLDAGSÁRÁS SPILLIFORRIT VEFVEIÐAR

Skrifaðu svörin þín hér:

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

Áfangi 4: Pörun hugtaka um öryggi

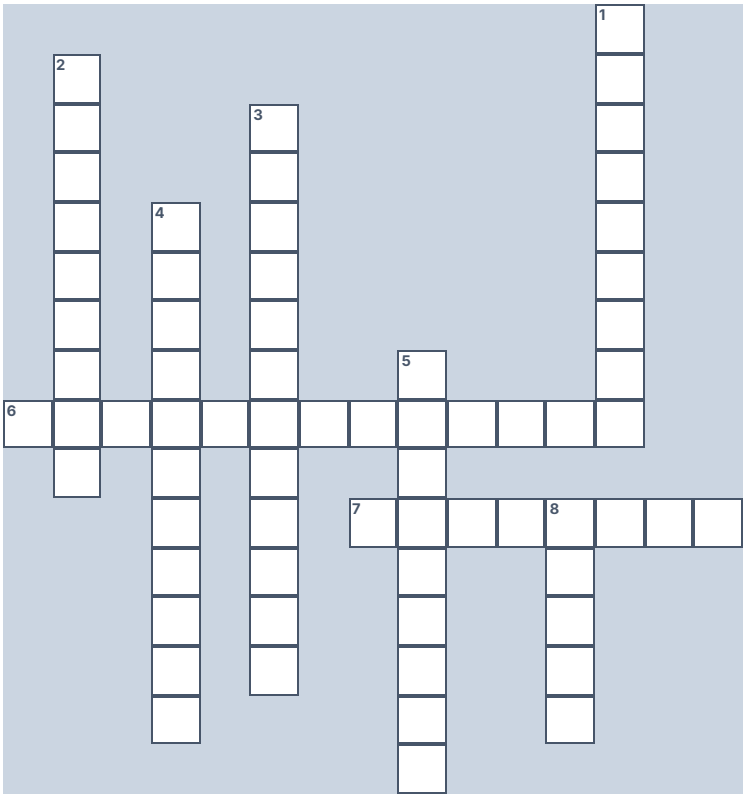
PÖRUN SKILGREININGA

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

☐	1. Gíslatökuhugbúnaðarógn	A	Skipulagðar leiðbeiningar á borð við NIST sem notaðar eru til að stýra netáhættu.
☐	2. Fjölþátta auðkenning	B	Skipulögð áætlun um meðhöndlun og takmörkun öryggisbrota.
☐	3. Núlldags-árás	C	Netvörn sem síar umferð eftir öryggisreglum.
☐	4. Gildruhunangskrukka	D	Spilliforrit sem dulkóða gögn og krefjast greiðslu fyrir afkóðun.
☐	5. Innbrotseldveggur	E	Veikleikaárás sem beinist að veikleika áður en framleiðandi gefur út öryggisuppfærslu.
☐	6. Viðbrögð við atvikum	F	Bestu starfsvenjur við stjórnun auðkenna og auðkenningarlykla.
☐	7. Lykilorðahreinlæti	G	Öryggisstaðfesting sem krefst tveggja eða fleiri auðkenningarþátta.
☐	8. Öryggisrammi	H	Tálbeitukerfi sem sett er upp til að lokka til sín og greina illgjarna aðila.

Áfangi 5: Krossgáta

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



LÁRÉTT

6. Tálkerfi sem sett er upp til að laða að og greina illgjarna aðila (13)

7. Skipulögð áætlun um meðhöndlun og takmörkun öryggisbrota (8)

LÓÐRÉTT

1. Öryggisstaðfesting sem krefst tveggja eða fleiri auðkenningarþátta (9)

2. Netvörn sem síar umferð eftir öryggisreglum (9)

3. Árás á veikleika áður en framleiðandi gefur út öryggisuppfærslu (12)

4. Spilliforrit sem dulkóðar gögn og krefst greiðslu fyrir afkóðun (11)

5. Bestu starfshættir við stjórnun auðkenna og auðkennislykla (9)

8. Skipulagðar leiðbeiningar á borð við NIST til að stýra netáhættu (5)

Áfangi 5, valkostur: Aðgengilegar vísbendingar fyrir krossgátu

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

LÁRÉTT

6 lárétt: Tálkerfi sem sett er upp til að laða að og greina illgjarna aðila (13 stafir):

7 lárétt: Skipulögð áætlun um meðhöndlun og takmörkun öryggisbrota (8 stafir):

LÓÐRÉTT

1 lóðrétt: Öryggisstaðfesting sem krefst tveggja eða fleiri auðkenningarþátta (9 stafir):

2 lóðrétt: Netvörn sem síar umferð eftir öryggisreglum (9 stafir):

3 lóðrétt: Árás á veikleika áður en framleiðandi gefur út öryggisuppfærslu (12 stafir):

4 lóðrétt: Spilliforrit sem dulkóðar gögn og krefst greiðslu fyrir afkóðun (11 stafir):

5 lóðrétt: Bestu starfshættir við stjórnun auðkenna og auðkennislykla (9 stafir):

8 lóðrétt: Skipulagðar leiðbeiningar á borð við NIST til að stýra netáhættu (5 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.

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

ORÐALISTI

GÍSLAFORRIT FJÖLÞÁTTA NÚLLDAGSÁRÁS HUNANGSKRUKKA ELDVEGGUR
VIÐBRÖGÐ HREINLÆTI RAMMI

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. GÍSLAFORRIT
B. FJÖLÞÁTTA
C. NÚLLDAGSÁRÁS
D. HUNANGSKRUKKA
E. ELDVEGGUR
F. VIÐBRÖGÐ
G. HREINLÆTI
H. RAMMI

SKILGREININGAR OG PÖRUNARREITIR

1. Netvörn sem síar umferð eftir öryggisreglum.
2. Skipulögð áætlun um meðhöndlun og takmörkun öryggisbrota.
3. Spilliforrit sem dulkóðar gögn og krefst greiðslu fyrir afkóðun.
4. Öryggisstaðfesting sem krefst tveggja eða fleiri auðkenningarþátta.
5. Bestu starfshættir við stjórnun auðkenna og auðkennislykla.
6. Skipulagðar leiðbeiningar á borð við NIST til að stýra netáhættu.
7. Árás á veikleika áður en framleiðandi gefur út öryggisuppfærslu.
8. Tálkerfi sem sett er upp til að laða að og greina illgjarna aðila.

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. AOIÍFRGRSTL
2. SÚDANRÁLSÁ GL
3. EGELGRVUD
4. NITIÆLHRE
5. TÞJAÁLFTÖ
6. NUSGKNKRHU KAA
7. VÐRÖGIBÐ
8. IRMMA

Aukaverkefni: Hugsaðu hratt

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

1	Störf í netöryggi			
2	Ástæður fyrir því að uppfæra hugbúnað			
3	Hlutir sem eldveggur getur lokað á			
4	Viðvörunarmerki í tölvupósti			
5	Hlutir sem þú afritar			
6	Þekktar tegundir netárása			
7	Hlutir sem hunangskrukka (honeypot) getur lokkað að			
8	Upplýsingar sem þú ættir aldrei að deila			
9	Merki þess að tölva sé sýkt			
10	Kvikmyndir eða þættir um tölvuþrjóta			
11	Öryggislög sem þú getur byggt upp			
12	Hlutir til að æfa í öryggisæfingu			
13	Öryggisverkfæri sem þú þekkir			
14	Fólk sem þú getur leitað til varðandi upplýsingatæknihjálp			
15	Orð sem byrja á „cyber“			

Áfangi 8: Dæmisögur um netöryggi

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

DÆMISAGA 1: ENDURHEIMTARÁÆTLUN EFTIR LAUSNARHUGBÚNAÐ



Aðstæður: Fyrirtækjanet er sýkt af kúgunarhugbúnaði sem læsir mikilvægum gagnagrunnum. Árásaraðilarnir krefjast $100,000 greiðslu í rafmynt. Fyrirtækið á afrit án nettengingar frá fyrir 24 klukkustundum.

Umræðuspurning: Greindu áhættuna af því að greiða og metðu endurheimtaráætlunina.

DÆMISAGA 2: VARNIR GEGN INNSKRÁNINGARFYLLINGU



Aðstæður: Netþjónusta verður fyrir lykilorðafyllingarárás (credential stuffing) þar sem tölvuþrjótar prófa milljónir para af notandanöfnum og lykilorðum sem stolið var frá öðrum vefsvæðum.

Umræðuspurning: Lýstu virkni þessarar árásar í smáatriðum og gerðu grein fyrir tveimur varnarkerfum.

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

25	23	31	10	10	6	26		15	7	23	9	12	6		34	12	25	25	
17	7	6		9	14	36	16	34	2	25	25	1							
1	26	6	15	7	18	18	12	18	10	26									

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: Hvert er meginmarkmið netöryggis?

Meginmarkmiðið er að vernda net, tæki og gögn gegn óheimilum aðgangi, árásum og óviljandi skemmdum.

Q2: Í hverju eru vefveiðar frábrugðnar markvissum vefveiðum (spear phishing)?

Vefveiðar eru víðtæk póstherferð sem beinist að tilviljanakenndum notendum, en markvissar vefveiðar (spear phishing) beinast að tilteknum einstaklingum með persónulegum upplýsingum.

Q3: Hvað er neteldveggur?

Eldveggur er netöryggiskerfi sem fylgist með og síar komandi og útgangandi umferð út frá fyrirfram skilgreindum öryggisreglum.

Q4: Hvers vegna er fjölþátta auðkenning (MFA) nauðsynleg?

MFA bætir við mikilvægu varnarlagi og kemur í veg fyrir aðgang jafnvel þótt árásaraðilar steli eða brjóti upp aðallykilorðið.

Q5: Hvað einkennir tölvuveiru?

Veira er spilliforrit sem afritar sig sjálft, festir sig við hreinar skrár og dreifist milli kerfa þegar það er keyrt.

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

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q6: Hvernig læsir gíslatökuforrit staðbundnum gögnum?

Gíslatökuforrit nota dulritunarreiknirit til að dulkóða skrár notenda svo að þær verði ólæsilegar þar til afkóðunarlykli er beitt.

Q7: Hvað er núlldagsveila (zero-day vulnerability)?

Zero-day er öryggisgalli í hugbúnaði sem söluaðilinn þekkir ekki, svo enginn tími gefst til að þróa bót áður en hann er nýttur.

Q8: Hvaða hlutverki gegnir NIST-rammi?

NIST-rammi veitir valfrjálsar leiðbeiningar og staðla til að hjálpa stofnunum að stýra og draga úr netöryggisáhættu.

Q9: Hvað er viðbragðsáætlun vegna öryggisatvika?

Það er skjalfest safn verklags til að greina, halda í skefjum og jafna sig eftir öryggisbrot og afhjúpun netsins.

Q10: Hvernig nýta félagsleg hjálparbrögð notendur?

Félagsleg hagræðing notar sálræna misnotkun til að blekkja starfsmenn til að gefa upp lykilorð eða sækja skaðlegar skrár.

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

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q1: Hvernig yfirbugar DDoS-árás vefþjóna?

DDoS-árás samhæfir milljónir sýktra tækja í botneti til að flæða netþjón með umferð og tæma bandvídd og örgjörvagetu.

Q2: Hver er munurinn á samhverfri og ósamhverfri dulkóðun?

Samhverf dulkóðun notar einn lykil til að dulkóða og afkóða, en ósamhverf dulkóðun notar par af opinberum og leynilegum lykli.

Q3: Hvernig framkvæma tölvuþrjótar SQL-innspýtingarárásir?

Árásarmenn setja skaðlegar SQL-skipanir í innsláttarreiti og blekkja bakenda gagnagrunninn til að gefa út óheimilar notendafærslur.

Q4: Hvað er hliðarhreyfing (lateral movement) í netárásum?

Það er aðferðin þar sem árásaraðilar nýta fyrsta aðgang að netþjóni til að brjótast inn í önnur samtengd kerfi á innra netinu.

Q5: Hvernig beinir DNS-fölsun (DNS spoofing) vefumferð annað?

DNS-fölsun breytir skyndiminnisfærslum nafnaþjóna og beinir venjulegum notendum á skaðlegar eftirlíkingar af vefsvæðum í stað raunverulegra léna.

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

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q6: Hvað er vélbúnaðaröryggislykill?

Það er raunverulegt tæki (eins og YubiKey) sem býr til dulritunarsannanir fyrir auðkenningu og veitir hámarksvörn gegn vefveiðum úr fjarlægð.

Q7: Hvernig nota öryggisteymi gildruþjóna (honeypots)?

Teymi setja upp gabbnetþjóna utan framleiðslu til að greina innrásir snemma og greina árásarmynstur óheimilla aðila.

Q8: Hver er meginreglan um lágmarksréttindi?

Það er öryggisstaðall sem takmarkar aðgangsréttindi notenda við algjört lágmark sem þarf til að sinna hlutverkum þeirra.

Q9: Hvernig misnotar millimaðurárás (Man-in-the-Middle) tengingar?

Árásaraðili hlerar og breytir samskiptum milli tveggja tækja á ódulkóðuðum netum og stelur lotutáknum og auðkennum.

Q10: Hvað eru vísbendingar um árás (IOC)?

IOC eru réttarfræðilegar vísbendingar, svo sem óvenjulegar breytingar á skrásetningu eða óviðkomandi IP-umferð, sem sýna að kerfi hafi verið brotist inn í.

Hluti 11: 10 staðreyndir um netöryggi og innsýn úr raunheimum

Farðu yfir raunverulegar staðreyndir um öryggisbrot, varnarkerfi og reglufylgnistaðla.

1. INNSÝN Í ÖRYGGI

Árásarmenn skanna netið stöðugt eftir berskjölduðum netþjónum og senda vefveiðapósta í pósthólf starfsfólks.

2. INNSÝN Í ÖRYGGI

Mannleg mistök, eins og að smella á vefveiðatengla, eru algengur þáttur í gagnaleka, og þess vegna skiptir þjálfun máli.

3. INNSÝN Í ÖRYGGI

Kostnaður vegna gagnaleka felur í sér lagalegar sektir, brottfall viðskiptavina, rannsókn og viðgerðir og getur numið milljónum dollara.

4. INNSÝN Í ÖRYGGI

Fjölþátta auðkenning sem stenst vefveiðar, svo sem vélbúnaðaröryggislyklar, er sterkasta gerð MFA og sá staðall sem CISA hvetur til. [2]

5. INNSÝN Í ÖRYGGI

Gíslatökuforrit eru áfram mikil ógn við fyrirtækjanet og CISA hvetur til afrita án nettengingar og dulkóðaðra afrita sem lykilvarnar. [4]

6. INNSÝN Í ÖRYGGI

Netöryggisrammi NIST 2.0 (2024) hefur sex kjarnaföll: Stjórna (Govern), Greina (Identify), Vernda (Protect), Finna (Detect), Bregðast við (Respond), Endurheimta (Recover). [1]

7. ÖRYGGISINNSÝN

Vélmenni sem stunda innskráningarfyllingu prófa leknar samsetningar notandanafns og lykilorðs í stórum stíl á innskráningargáttum banka og netverslana.

8. ÖRYGGISINNSÝN

Markaðir fyrir zero-day veikleika eru til um allan heim, þar sem alvarlegir veikleikar geta selst fyrir háar fjárhæðir áður en þeir eru lagfærðir.

9. ÖRYGGISINNSÝN

Hunangsgildra (honeypot) tilkynnir um innbrot strax þar sem lögmætir notendur hafa enga ástæðu til að nálgast hana.

10. INNSÝN Í ÖRYGGI

Transport Layer Security (TLS) dulkóðar vafralotur og kemur í veg fyrir pakkahleranir á opinberum Wi-Fi netum.

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] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] 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

[4] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Lausnir: Áfangi 1 – Fjölval

1 **Vefveiðaárásir** VEFVEIÐAR **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Vefveiðaherferðir reyna að stela auðkennisupplýsingum og viðkvæmum notendagögnum með fölsuðum tölvupósti. Heimild: OWASP Secure Configuration.

2 **Reikningsvernd** MFA-LYKILL **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Fjölþátta auðkenning (MFA) með vélbúnaðarlyklum veitir sterkustu vörn fyrir aðgang að reikningum. Heimild: NIST Digital Identity.

3 **Ógn af gíslatökuforritum** GÍSLATÖKUFORRIT **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Gíslatökuforrit dulkóða mikilvæg kerfi og gögn og krefjast greiðslu í rafmynt fyrir afkóðunarlykla. Heimild: Center for Internet Security (CIS).

4 **Zero-day veikleiki** ZERO-DAY **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Zero-day ógnir nýta ólagfærða, óþekkta öryggisgalla áður en framleiðandi gefur út lagfæringu. Tilvitnun: OWASP Secure Configuration.

5 **Öryggisrammar** RAMMAVERK **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Rammar á borð við NIST veita skipulagðar leiðbeiningar sem hjálpa stofnunum að stýra netáhættu og draga úr henni. Heimild: NIST Digital Identity.

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Markviss vefveiði** VEFVEIÐAR — **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Vefveiðaárásir beinast bæði að fyrirtækjanetum og einkareikningum til að auka árásarleiðir. Heimild: OWASP Secure Configuration.

7 **Spurning 7** — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

MFA krefst annars þáttar og því nægir stolið lykilorð eitt og sér yfirleitt ekki til að skrá sig inn.

8 **Umferðareldveggur** ELDVEGGUR — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Eldveggir skoða umferð og loka á hana um tilteknar netgáttir til að sía burt óheimilar tengingar. Heimild: Center for Internet Security (CIS).

9 **Viðbrögð við zero-day** ZERO-DAY — **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Að lagfæra núlldagaveilur krefst kóðaleiðréttinga og WAF-síunar þar sem undirskriftir eru ekki enn til. Heimild: OWASP Secure Configuration.

10 **Gildruþjónar** HUNANGSKRUKKA — **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Hunangskrukkur (honeypots) eru blekkingarnetþjónar sem öryggisteymi nota til að tæla, vara við og rannsaka illgjarna aðila. Heimild: Center for Internet Security (CIS).

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

D 1. Gíslatökuhugbúnaðarógn	G 2. Fjölþátta auðkenning	E 3. Núlldags-árás	H 4. Gildruhunangskrukka
C 5. Innbrotseldveggur	B 6. Viðbrögð við atvikum	F 7. Lykilorðahreinlæti	A 8. Öryggisrammi

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

1 ELDVEGGUR	2 NÚLLDAGSÁRÁS	3 VEFVEIÐAR	4 SPILLIFORRIT
5 HREINLÆTI	6 DULKÓÐUN		

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

1 E – ELDVEGGUR	2 F – VIÐBRÖGÐ	3 A – GÍSLAFORRIT	4 B – FJÖLÞÁTTA
5 G – HREINLÆTI	6 H – RAMMI	7 C – NÚLLDAGSÁRÁS	8 D – HUNANGSKRUKKA

UMRÆÐUATRIÐI FYRIR KENNARA

Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt Gíslatökuhugbúnaðarógn, Fjölþátta auðkenning og Núlldags-árás með eigin orðum og gefið dæmi um hvert hugtak.

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

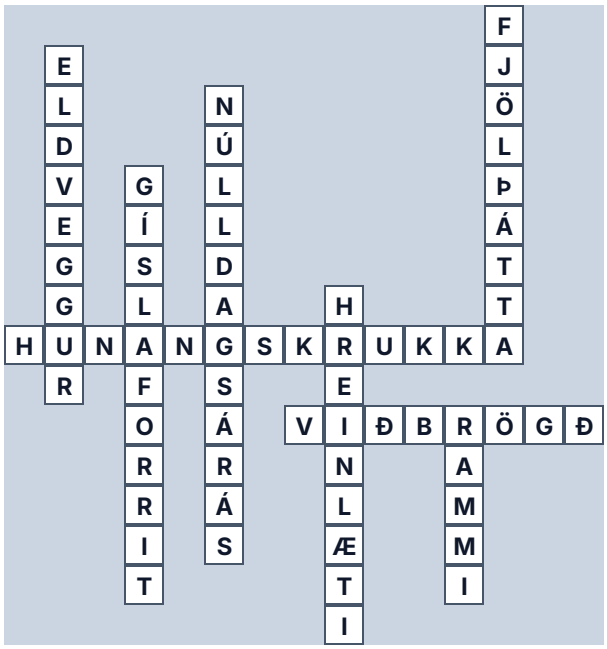
Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR

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

LAUSN KROSSGÁTUNNAR



LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

LÁRÉTT

6 lárétt: HUNANGSKRUKKA Tálkerfi sem sett er upp til að laða að og greina illgjarna aðila (13 stafir)

7 lárétt: VIÐBRÖGÐ Skipulögð áætlun um meðhöndlun og takmörkun öryggisbrota (8 stafir)

LÓÐRÉTT

1 lóðrétt: FJÖLÞÁTTA Öryggisstaðfesting sem krefst tveggja eða fleiri auðkenningarþátta (9 stafir)

2 lóðrétt: ELDVEGGUR Netvörn sem síar umferð eftir öryggisreglum (9 stafir)

3 lóðrétt: NÚLLDAGSÁRÁS Árás á veikleika áður en framleiðandi gefur út öryggisuppfærslu (12 stafir)

4 lóðrétt: GÍSLAFORRIT Spilliforrit sem dulkóðar gögn og krefst greiðslu fyrir afkóðun (11 stafir)

5 lóðrétt: HREINLÆTI Bestu starfshættir við stjórnun auðkenna og auðkennislykla (9 stafir)

8 lóðrétt: RAMMI Skipulagðar leiðbeiningar á borð við NIST til að stýra netáhættu (5 stafir)

Lausnir: Stafaruglingur og dulmál

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

LYKILL ORÐARAÐAR

1. A O I Í F R G R S T L — GÍSLAFORRIT
2. S Ú D A N R Á L S Á G L — NÚLLDAGSÁRÁS
3. E G E L G R V U D — ELDVEGGUR
4. N I T I Æ L H R E — HREINLÆTI
5. T Þ J A Á L F T Ö — FJÖLÞÁTTA
6. N U S G K N K R H U K A A — HUNANGSKRUKKA
7. V Ð R Ö G I B Ð — VIÐBRÖGÐ
8. I R M M A — RAMMI

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"TRYGGÐU KERFIÐ ÞITT MEÐ FJÖLÞÁTTA AUÐKENNINGU"

Lausnir dæmisagna

A Dæmisaga 1: Endurheimtaráætlun eftir lausnarhugbúnað

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Net fyrirtækis er sýkt af gagnagíslatökuforriti sem læsir mikilvægum gagnagrunnum. Árásaraðilarnir krefjast $100,000 greiðslu í rafmynt. Fyrirtækið á ótengd afrit frá fyrir 24 klukkustundum.
- Ráðlögð aðferð og lausn: Hættur við greiðslu: Greiðsla tryggir ekki afkóðun skráa, merkir fyrirtækið sem skotmark sem borgar og fjármagnar glæpastarfsemi. Endurheimtaraðferð: Teymið ætti að einangra sýkta hýsla, hreinsa netþjóna í hættu og endurheimta gögn úr ótengdum afritum. Það verður að lagfæra upphaflegu aðgangsleiðina (vefveiðar eða veilu) til að koma í veg fyrir tafarlausa endursýkingu.

B Dæmisaga 2: Varnir gegn innskráningarfyllingu

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Aðstæður til greiningar: Netþjónusta verður fyrir árás með innskráningarfyllingu (credential stuffing) þar sem tölvuþrjótar prófa milljónir notandanafna og lykilorða sem var stolið af öðrum vefjum.
- Ráðlögð aðferð og lausn: Aðferð: Árásaraðilar nýta endurnotkun lykilorða á milli vefsvæða með sjálfvirkum vélmennum til að skrá sig inn á notendaaðganga. Varnir: 1. Fjölþátta auðkenning (MFA) stöðvar innskráningartilraunir jafnvel þótt lykilorðið sé rétt. 2. Hraðatakmarkanir og CAPTCHA stöðva sjálfvirka vélmennaumferð sem flæðir yfir innskráningarslóðir.