Nafn: _____ Dagsetning: _____ Stig: _____

Zero Trust-arkitektúr og öryggi

Stöðug sannprófun, örskipting netsins, auðkenna- og aðgangsstjórnun, lágmarksheimildir og stöðuathuganir.

YFIRLIT UM NÁM Í ZERO TRUST-ÖRYGGI

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 Zero Trust-arkitektúr og -öryggi. Þú kynnist stöðugri sannprófun, örskiptingu nets, auðkenna- og aðgangsstjórnun (IAM), lágmarksheimildum og lotuúttektum.

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/null-traust-netoryggi/

Námsvegvísir þinn: Zero Trust-stefna

- Skildu kjarnareglu stöðugrar sannprófunar.
- Innleiddu örskiptingu nets og aðgang með lágmarksréttindum.
- Stilltu stöðuathuganir tækja og virka úttekt á setum.

LEIÐBEININGAR UM ZERO TRUST-ÖRYGGI

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

ZERO TRUST-ARKITEKTÚR OG ÖRYGGI (INNGANGUR)

Zero Trust-öryggi kemur í stað gamalla jaðarlíkana netsins með ströngri stefnu um að treysta aldrei og staðfesta alltaf. Örskipting netsins, auðkennis- og aðgangsstjórnun (IAM), lágmarksréttindi og stöðuathuganir koma í veg fyrir hliðarhreyfingu ógna.

LESTU HVERN ÁFANGA VANDLEGA OG VELDU EÐA SKRIFAÐU RÉTT SVAR.

Áfangi 1: Fjölvalsáskorun

1 **1. Hver er grundvallarregla Zero Trust-öryggis?**

- A. Treystu aldrei, staðfestu alltaf hverja aðgangsbeiðni óháð uppruna
- B. Að gera ráð fyrir að öll umferð innan eldveggs fyrirtækisins sé örugg
- C. Að geyma gagnagrunnsskrár ódulkóðaðar til að auka hraða
- D. Að framfylgja auðkenningu tölvupósts eingöngu með SPF-færslum

2 **2. Hvað er örskipting netkerfis (network micro-segmentation)?**

- A. Að skipta netum í lítil, einangruð svæði til að hefta hliðlæga útbreiðslu
- B. Að dulkóða netkort meðan gögn eru í flutningi
- C. Að tengja alla staðbundna netþjóna við eina opinbera IP-tölu
- D. Að fylgjast með lyklaborðsinnslætti notenda í vafralotum

3 **3. Hver er grundvallarregla minnstu réttinda (principle of least privilege)?**

- A. Að takmarka aðgangsheimildir notenda við það sem er nauðsynlegt fyrir starf þeirra
- B. Að veita öllum notendum öll kerfisréttindi sjálfgefið
- C. Að leyfa nafnlausar innskráningar á gagnagrunnsnetþjóna fyrirtækis
- D. Að stilla opinbera Wi-Fi-bein án lykilorða

4 **4. Hvað er auðkenna- og aðgangsstýring (Identity and Access Management, IAM)?**

- A. Rammar sem stýra stafrænum auðkennum og stjórna kerfisréttindum
- B. Vírusvarnartól sem skanna skráamöppur á staðnum
- C. Afritunarkerfi sem notar miðla án nettengingar (air-gapped)
- D. Gáttarsamskiptaregla fyrir tölvupóst sem hafnar fölsuðum lénum

5 **5. Hvað merkir stöðug auðkenning?**

- A. Að sannreyna ítrekað auðkenni notanda og stöðu tækis í virkri lotu
- B. Að skipta um aðallykilorð á 10 mínútna fresti
- C. Að tætigilda gagnagrunnsfærslur með mörgum reikniritum
- D. Að dulkóða netflutningspakka með TLS-lyklum

Áfangi 2: Satt eða ósatt

6 Spurning 6

6. Zero Trust gerir ráð fyrir að öll umferð innan eldveggs fyrirtækisins sé örugg.

Satt Ósatt

7 Spurning 7

7. Örskipting dregur úr getu árásaraðila til að færa sig til hliðar milli innri netþjóna.

Satt Ósatt

8 Spurning 8

8. Lágmarksréttindi veita sjálfgefið aðgang að öllum gagnagrunnsskrám.

Satt Ósatt

9 Spurning 9

9. Stöðug sannprófun staðfestir heilbrigði tækis og innskráningarupplýsingar í gegnum alla innskráningarsetu.

Satt Ósatt

10 Spurning 10

10. Innleiðing Zero Trust dregur úr áhrifum þess að innskráningarupplýsingar fyrirtækis séu afhjúpaðar.

Satt Ósatt

Áfangi 3: Lykilhugtök fyllt inn

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

1. Að krefjast skilríkja við hvern aðgangspunkt er samfelld _____ .
2. Að skipta fyrirtækjanetinu í örsmá svæði kallast _____ .
3. Stafræn auðkenni og aðgangsstýring eru stillt í kerfi sem kallast _____ .
4. Takmörkun á heimildum notenda byggir á meginreglunni um sem fæst _____ .
5. Mat á heilbrigði tengdra tækja felst í að skanna _____ þeirra.
6. Skráning og rýni virkra lota er sá liður öryggismála sem kallast _____ .

ORÐABANKI

BEINIR ELDVEGGUR IAM-KERFI RÉTTINDI STAÐFESTING ÚTTEKT
ÖRSKIPTING ÖRYGGISÁSTAND

Skrifaðu svörin þín hér:

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

Áfangi 4: Pörun hugtaka um öryggi

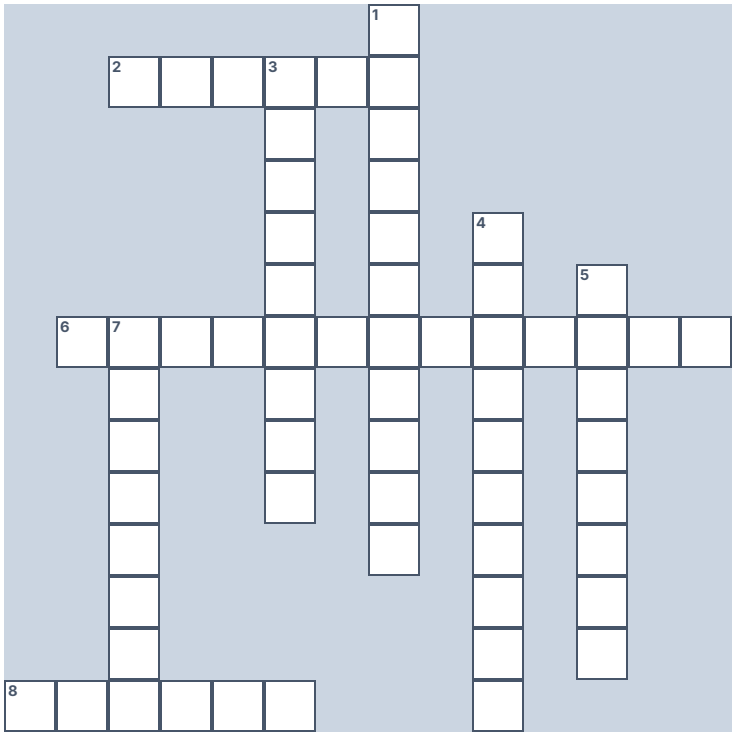
PÖRUN SKILGREININGA

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

☐	1. STAÐFESTING	A	Stjórnun aðgangs að innskráningarupplýsingum notenda.
☐	2. SKIPTING	B	Meginreglan um lágmarksaðgangsréttindi.
☐	3. IAM	C	Að leiða netpakkaumferð.
☐	4. RÉTTINDI	D	Vörn ytri netmarka.
☐	5. ÖRYGGISSTAÐA	E	Yfirferð á skráðum aðgangslotum.
☐	6. ENDURSKOÐUN	F	Skipting innri netsvæða.
☐	7. ELDVEGGUR	G	Alltaf að athuga auðkenni notenda.
☐	8. BEINIR	H	Mat á heilbrigði tækis.

Áfangi 5: Krossgáta

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



LÁRÉTT

2. Rýni í skráðar aðgangslotur (6)

6. Mat á heilbrigði tækja (13)

8. Beinir umferð netpakka (6)

LÓÐRÉTT

1. Skilríki notenda eru alltaf athuguð (11)

3. Vörn ytri netjaðars (9)

4. Skipting innri netsvæða (10)

5. Stjórnun á aðgangi að notendaskilríkjum (8)

7. Meginreglan um minnstu aðgangsréttindi (8)

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: Rýni í skráðar aðgangslotur (6 stafir):

6 lárétt: Mat á heilbrigði tækja (13 stafir):

8 lárétt: Beinir umferð netpakka (6 stafir):

LÓÐRÉTT

1 lóðrétt: Skilríki notenda eru alltaf athuguð (11 stafir):

3 lóðrétt: Vörn ytri netjaðars (9 stafir):

4 lóðrétt: Skipting innri netsvæða (10 stafir):

5 lóðrétt: Stjórnun á aðgangi að notendaskilríkjum (8 stafir):

7 lóðrétt: Meginreglan um minnstu aðgangsréttindi (8 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 T Ö U É R X Ö É A A R Ó N P
G I Ú Þ R J S R Ú T E D N Æ B
N F R F T Ý Y S Í A L S Ö Æ Æ
I R I K Ú F I K M S D J L L U
T E N Ó T G P I R G V Ö A O X
S K I F T V B P Æ T E Æ Á G L
E M E Ö E G J T O P G N Ý B L
F A B Ö K Æ F I Þ Ó G Y V K V
Đ I P Á T O X N Ú L U G X D Þ
A V J S Á Ý Ö G Þ M R T R Ý I
T Ö R Y G G I S Á S T A N D Ó
S Đ A D J R Y Ý Ý K Í H Ú H F
Á É R É T T I N D I I K U T Y
S Ö E H É T D A L P B Ö M J X
S V A T Ý J M M G H N H S F K

ORÐALISTI

STAÐFESTING ÖRSKIPTING IAMKERFI RÉTTINDI ÖRYGGISÁSTAND ÚTTEKT
ELDVEGGUR BEINIR

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. STAÐFESTING
B. ÖRSKIPTING
C. IAMKERFI
D. RÉTTINDI
E. ÖRYGGISÁSTAND
F. ÚTTEKT
G. ELDVEGGUR
H. BEINIR

SKILGREININGAR OG PÖRUNARREITIR

1. Vörn ytri netjaðars. ____
2. Rýni í skráðar aðgangslotur. ____
3. Meginreglan um minnstu aðgangsréttindi. ____
4. Skipting innri netsvæða. ____
5. Beinir umferð netpakka. ____
6. Mat á heilbrigði tækja. ____
7. Stjórnun á aðgangi að notendaskilríkjum. ____
8. Skilríki notenda eru alltaf athuguð. ____

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. **FSNTETSIAGÐ** _____
2. **KIIAFREM** _____
3. **RÖÁTSNDYSGIAG** _____
4. **ERUVGGELD** _____
5. **IPGRKTIÖNS** _____
6. **DITNRIÉT** _____
7. **KÚETTT** _____
8. **IRBINE** _____

Aukaverkefni: Hugsaðu hratt

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

1	Upplýsingar sem þú ættir aldrei að deila			
2	Öruggar venjur sem þú getur byrjað á í dag			
3	Hlutir sem eru athugaðir á tæki			
4	Hlutir sem eru skráðir í atburðaskrá			
5	Orð tengd netöryggi			
6	Hlutir sem Zero Trust athugar			
7	Staðir þar sem þú sýnir skilríki í daglegu lífi			
8	Leiðir til að sanna að það sért í raun þú			
9	Hlutir til að gera eftir gagnaleka			
10	Merki þess að tölva sé sýkt			
11	Ástæður fyrir því að uppfæra hugbúnað			
12	Aðgangsstig í fyrirtæki			
13	Öryggisverkfæri sem þú þekkir			
14	Svæði sem hægt er að skipta neti í			
15	Málshættir um traust			

Áfangi 8: Dæmisögur um netöryggi

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

DÆMISAGA 1: YFIRFÆRSLA Í ZERO TRUST-NETARKITEKTÚR



Aðstæður: Stórfyrirtæki notar nú flatt innra net þar sem hvaða tæki sem er á staðarnetinu getur nálgast alla fyrirtækjanetþjóna og gagnagrunna.

Umræðuspurning: Hannaðu örskiptingarstefnu fyrir net til að takmarka hliðlæga hreyfingu.

DÆMISAGA 2: INNLEIÐING AÐGANGSSTÝRINGA MEÐ LÁGMARKSHEIMILDUM



Aðstæður: Úttektarskrár sýna að tímabundnir gagnagrunnsnotendur og lægra settir starfsmenn hafa víðtæk lestrar- og skrifréttindi að mikilvægum bókhaldsgagnagrunnum.

Umræðuspurning: Gerðu úttekt á IAM-réttindum í gagnagrunni og takmarkaðu þau til að framfylgja lágmarksréttindum.

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

24	25	1	6	9	7	24	25	26		1	16	16	25	1	9		17	7	6
18	**27**	**16**	**16**	**25**	**23**	**1**	**26**	**24**	**25**	**12**		**13**		**36**	**23**	**31**	**10**	**10**	**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 Zero Trust?

Zero Trust er öryggisrammi sem gerir ráð fyrir að ógnir séu til bæði utan og innan netmarkanna og krefst staðfestingar fyrir hverja beiðni. [1]

Q2: Hver er kjarnareglan í Zero Trust?

Treystu aldrei, staðfestu alltaf.

Q3: Hvað er örskipting (micro-segmentation)?

Að skipta neti í lítil, örugg rökleg hólf til að stýra umferð og afmarka öryggisbrot.

Q4: Hvað er lágmarksréttindi (least privilege)?

Að veita notendum aðeins lágmarksaðgangsréttindi sem þarf til að sinna tilteknum verkefnum þeirra. [2]

Q5: Fyrir hvað stendur IAM?

Auðkenna- og aðgangsstýring (Identity and Access Management).

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

Farðu yfir algengar spurningar og svör um varnir gegn netógnum.

Q6: Hvernig hjálpar stöðuathugun tækis?

Það staðfestir að tæki sé uppfært, með virka veiruvörn og öruggt áður en aðgangur er veittur.

Q7: Hvað er hliðarhreyfing (lateral movement)?

Aðferðin sem árásaraðilar nota til að fikra sig um net frá fyrsta sýkta hnút yfir í verðmætari kerfi.

Q8: Kemur Zero Trust í stað eldveggja?

Nei, það styrkir þær með því að bæta við auðkennismiðuðum athugunum og innri skiptingareldveggjum.

Q9: Hvað er stöðug sannvottun?

Stöðug sannvottun á auðkenni notanda allan innskráningartímann, ekki aðeins við fyrstu innskráningu.

Q10: Hvers vegna er flatt net hættulegt?

Í flötum netum gerir einn afhjúpaður hnútur árásaraðilum auðvelt að komast í hvaða gagnagrunn sem er á netinu.

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

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q1: Hvernig tekur Zero Trust á jaðarmódelinu?

Það kemur í stað úrelta „kastala og vallargrafar“ líkansins og færir vörn frá jaðarnetum yfir á tiltekin notendaauðkenni og auðlindir.

Q2: Hvað er stefnuákvörðunarpunktur (PDP)?

Kerfishlutinn sem metur heimildarbeiðnir gagnvart öryggisreglum til að ákveða hvort veita skuli aðgang.

Q3: Hvað er stefnuframfylgdarpunktur (PEP)?

Kerfishnúturinn (eins og gátt eða miðlari) sem leyfir eða hafnar tengibeiðnum í reynd á grundvelli ákvörðunar PDP.

Q4: Hvernig styður hlutverkamiðuð aðgangsstýring (RBAC) Zero Trust?

RBAC flokkar heimildir í tiltekin hlutverk, sem hjálpar til við að koma í veg fyrir að notendur erfi óhófleg stjórnendaréttindi.

Q5: Hvað er samhengisbundin aðgangsstýring?

Mat á innskráningarbeiðnum með aukavísbendingum eins og landfræðilegri staðsetningu, stöðu tækis og innskráningartíma til að meta áhættu.

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

Kannaðu ítarlega tæknilega þætti öryggisrammaverka, spilliforritagreiningar og gagnareglufylgni.

Q6: Hvernig er örskipting (micro-segmentation) frábrugðin hefðbundnum VLAN?

VLAN skipta netum í breiðar rökrænar einingar á lagi 2, en örskipting notar hugbúnaðarstefnu til að einangra einstök vinnuálag.

Q7: Hvað er aðgangur á réttum tíma (just-in-time, JIT)?

Að veita tímabundið aukin stjórnendaréttindi og afturkalla þau sjálfkrafa þegar verkefninu er lokið.

Q8: Hvernig tryggir þú API-viðmót innan Zero Trust-ramma?

Með því að krefjast dulritunarlega undirritaðra OAuth-tákna og úttektar á undirskriftum beiðna við hverja API-gátt.

Q9: Hvað er biðlari fyrir Zero Trust-netaðgang (ZTNA)?

Hugbúnaðarmiðlari sem kemur á öruggum, dulkóðuðum útgangandi tengingum við tiltekin forrit frekar en hrá undirnet.

Q10: Hvernig hjálpar skráaúttekt Zero Trust?

Stöðug skráning gerir sjálfvirkum öryggisgreiningartólum kleift að greina frávik og stöðva strax grunsamlegar innskráningar.

Hluti 11: 10 staðreyndir um netöryggi og innsýn úr raunheimum

Farðu yfir raunverulegar staðreyndir um öryggisbrot, varnarkerfi og reglufylgnistaðla.

1. INNSÝN Í ÖRYGGI

Zero Trust-arkitektúr kemur í stað gamla kastala-og-síkis-líkansins með staðfestingarreglum sem miðast við auðkenni.

2. INNSÝN Í ÖRYGGI

Netörskipting minnkar svæðið sem spilliforrit nær til með því að einangra vinnuálag í litlum vernduðum svæðum.

3. INNSÝN Í ÖRYGGI

Zero Trust leggur áherslu á að vernda auðlindir eins og eignir, þjónustu og reikninga frekar en netskiptingar. [1]

4. INNSÝN Í ÖRYGGI

Stefnur um lágmarksréttindi draga úr hættu á að innanbúðarmenn taki gögn út úr kjarnagagnagrunnum.

5. INNSÝN Í ÖRYGGI

Stöðusannprófun tækja athugar plástrastig stýrikerfis og stöðu virkrar vírusvarnar í rauntíma.

6. INNSÝN Í ÖRYGGI

ZTNA-miðlarar (Zero Trust Network Access) geta komið í stað fyrirtækja-VPN eða bætt þau upp til að takmarka umfang aðgangs notenda.

7. ÖRYGGISINNSÝN

Framsal stjórnendaréttinda á réttum tíma (Just-in-Time, JIT) dregur úr hættu á þjófnaði aðgangsupplýsinga á lénsstýringum.

8. ÖRYGGISINNSÝN

Stöðug sannprófun skráir og skoðar hegðun setu og stöðvar notendur sem sýna óeðlilegt mynstur í skriftukeyrslu.

9. ÖRYGGISINNSÝN

Hefðbundnar jaðarvarnir stöðva ekki hliðlægar árásir þegar stjórnandaauðkenni lekur.

10. INNSÝN Í ÖRYGGI

NIST Special Publication 800-207 (2020) gefur óhlutbundna skilgreiningu á Zero Trust-arkitektúr, ásamt innleiðingarlíkönum. [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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

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

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

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

Lausnir: Áfangi 1 – Fjölval

1 **Spurning 1** **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hver er grundvallarregla Zero Trust-öryggis? → Treystu aldrei, staðfestu alltaf hverja aðgangsbeiðni óháð uppruna

2 **Spurning 2** **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað er örskipting netkerfis (network micro-segmentation)? → Að skipta netum í lítil, einangruð svæði til að hefta hliðlæga útbreiðslu

3 **Spurning 3** **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hver er grundvallarregla minnstu réttinda (principle of least privilege)? → Að takmarka aðgangsheimildir notenda við það sem er nauðsynlegt fyrir starf þeirra

4 **Spurning 4** **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað er auðkenna- og aðgangsstýring (Identity and Access Management, IAM)? → Rammar sem stýra stafrænum auðkennum og stjórna kerfisréttindum

5 **Spurning 5** **Rétt svar: A**

ATHUGASEMD FYRIR KENNARA

Hvað merkir stöðug auðkenning? → Að sannreyna ítrekað auðkenni notanda og stöðu tækis í virkri lotu

Lausnir: Áfangi 2 – Satt eða ósatt

6 **Spurning 6** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: Zero Trust veitir ekkert óbeint traust byggt á staðsetningu í neti, innan eða utan þess.

7 **Spurning 7** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Satt: litlar einangraðar einingar takmarka hversu langt boðflenna getur fært sig milli netþjóna.

8 **Spurning 8** **Rétt svar: Ósatt**

ATHUGASEMD FYRIR KENNARA

Ósatt: lágmarksréttindi veita aðeins þann lágmarksaðgang sem hvert hlutverk þarf.

9 **Spurning 9** **Rétt svar: Satt**

ATHUGASEMD FYRIR KENNARA

Stöðug sannprófun staðfestir heilbrigði tækis og innskráningarupplýsingar í gegnum alla innskráningarsetu.

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

ATHUGASEMD FYRIR KENNARA

Innleiðing Zero Trust dregur úr áhrifum þess að innskráningarupplýsingar fyrirtækis séu afhjúpaðar.

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

G 1. STAÐFESTING	F 2. SKIPTING	A 3. IAM	B 4. RÉTTINDI
H 5. ÖRYGGISSTAÐA	E 6. ENDURSKOÐUN	D 7. ELDVEGGUR	C 8. BEINIR

ÁFANGI 3: LAUSNIR – LYKILHUGTÖK

1 STAÐFESTING	2 ÖRSKIPTING	3 IAM-KERFI	4 RÉTTINDI
5 ÖRYGGISÁSTAND	6 ÚTTEKT		

ÁFANGI 6, VALKOSTUR: LAUSNIR – PÖRUN ORÐA

1 G – ELDVEGGUR	2 F – ÚTTEKT	3 D – RÉTTINDI	4 B – ÖRSKIPTING
5 H – BEINIR	6 E – ÖRYGGISÁSTAND	7 C – IAMKERFI	8 A – STAÐFESTING

UMRÆÐUATRIÐI FYRIR KENNARA

Lykilhugtök:
Athugaðu hvort nemendur geti útskýrt STAÐFESTING, SKIPTING og IAM með eigin orðum og gefið dæmi um hvert hugtak.

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

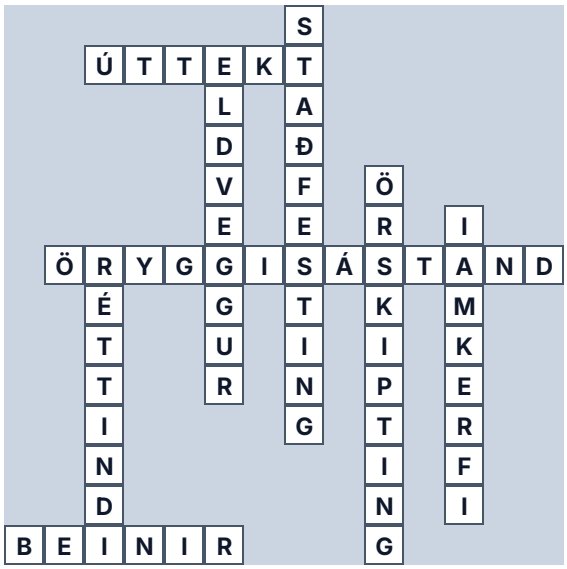
Mat á heimildum:
Biddu nemendur að sannreyna að minnsta kosti eina fullyrðingu í heimildum blaðsins og ræðið hvers vegna tölur, verð og reglur geta breyst með tímanum.

Lausnir við þrautum og athugasemdir fyrir kennara

LAUSN ORÐALEITAR

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

LAUSN KROSSGÁTUNNAR



LEIÐBEININGAR FYRIR KENNARA UM LAUSNIR KROSSGÁTU

LÁRÉTT

2 lárétt: ÚTTEKT Rýni í skráðar aðgangslotur (6 stafir)

6 lárétt: ÖRYGGISÁSTAND Mat á heilbrigði tækja (13 stafir)

8 lárétt: BEINIR Beinir umferð netpakka (6 stafir)

LÓÐRÉTT

1 lóðrétt: STAÐFESTING Skilríki notenda eru alltaf athuguð (11 stafir)

3 lóðrétt: ELDVEGGUR Vörn ytri netjaðars (9 stafir)

4 lóðrétt: ÖRSKIPTING Skipting innri netsvæða (10 stafir)

5 lóðrétt: IAMKERFI Stjórnun á aðgangi að notendaskilríkjum (8 stafir)

7 lóðrétt: RÉTTINDI Meginreglan um minnstu aðgangsréttindi (8 stafir)

Lausnir: Stafaruglingur og dulmál

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

LYKILL ORÐARAÐAR

1.	F S N T E T S I A G Đ	STAÐFESTING	5.	I P G R K T I Ö N S	ÖRSKIPTING
2.	K I I A F R E M	IAMKERFI	6.	D I T N R I É T	RÉTTINDI
3.	R Ö Á T S N D Y S G I A G	ÖRYGGISÁSTAND	7.	K Ú E T T T	ÚTTEKT
4.	E R U V G G E L D	ELDVEGGUR	8.	I R B I N E	BEINIR

LYKILL AÐ LEYNIDULMÁLSÞRAUT

"STAÐFESTU ALLTAF MEÐ NÚLLTRAUSTI Í ÖRYGGI"

Lausnir dæmisagna

A Dæmisaga 1: Yfirfærsla í Zero Trust-netarkitektúr

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Greining aðstæðna: Stórt fyrirtæki notar nú flatt innra net þar sem hvaða tæki sem er á staðarnetinu hefur aðgang að öllum netþjónum og gagnagrunnum fyrirtækisins.
- Ráðlögð aðferð og lausn: Skiptu flata netinu í einangruð svæði eftir deildum. Settu upp innri eldveggi til að stýra umferð milli svæða og gerðu staðfestingu tengingartákna að skilyrði fyrir öllum aðgangi.

B Dæmisaga 2: Innleiðing aðgangsstýringa með lágmarksheimildum

Lausn fyrir kennara

VIÐMIÐ VIÐ EINKUNNAGJÖF

Svör nemenda ættu að ná yfir eftirfarandi atriði:

- Aðstæður til greiningar: Úttektarannálar sýna að tímabundnir gagnagrunnsnotendur og starfsmenn á lágu stigi hafa almennar lestrar- og skrifheimildir að mikilvægum bókhaldsgagnagrunnum.
- Ráðlögð aðferð og lausn: Afturkallaðu öll altæk stjórnendaréttindi. Innleiddu hlutverkamiðaða aðgangsstýringu (RBAC) sem svarar nákvæmlega til starfshlutverka og komdu á vikulegum sjálfvirkum yfirferðum á heimildum.