Navn: _____ Dato: _____ Point: _____

Grundlæggende cybersikkerhed og forebyggelse af trusler

Cybersikkerhedstrusler, netværksfirewalls, multifaktorgodkendelse (MFA), sikkerhedsrammeværker

OVERBLIK OVER GRUNDLÆGGENDE CYBERSIKKERHED

SIKRET

DATAKRYPTERING

256-bit AES-standard

OVERHOLDER KRAV

GLOBALE STANDARDER

GDPR- og CCPA-rammer

ZERO-TRUST

ADGANGSPOLITIK

Multifaktorgodkendelse

Velkommen! Dette opgavehæfte guider dig gennem grundprincipperne i cybersikkerhed og forebyggelse af trusler online. Du vil udforske malware, flerfaktorgodkendelse, firewalls og rammer for hændelsesberedskab.

OPGAVEARKETS KONTROLPUNKTER

- [ ] **Del 1-4: Lær cybersikkerhed og trusselsforebyggelse.**
- [ ] **Del 5-7: Løs kryds og tværs samt ordjagt.**
- [ ] **Del 8-9: Løs casestudier og chifferudfordring.**
- [ ] **Del 10: Gennemgå grundlæggende og avanceret FAQ.**
- [ ] **Del 11: Udforsk 10 interessante fakta fra virkeligheden.**
- [ ] **Bonus: Tænk hurtigt-udfordring.**

Åbn VPN.com's guide til cybersikkerhed

URL: https://www.vpn.com/da/cybersikkerhed/

Din læringsplan for grundlæggende cybersikkerhed

- Genkend de almindelige veje for malware, phishing og indtrængen i virksomhedens netværk.
- Indfør standardkontroller som MFA, firewalls og beskyttelse af endepunkter.
- Vurdér procedurer for hændelsesberedskab, der begrænser skaden ved databrud.
- Analysér organisationens risici og sikkerhed i forhold til NIST's retningslinjer.
- Indfør god sikkerhedshygiejne mod automatiske angreb med lækkede adgangskoder.

VEJLEDNING TIL GUIDEN OM CYBERSIKKERHED

Besvar flervalgs- og sandt/falsk-spørgsmålene, udfyld sætningerne med ord fra ordbanken, match definitionerne, og løs kryds og tværs samt ordjagten. Anvend din viden om forebyggelse af trusler. Slut af med bonusaktiviteten Tænk hurtigt.

GRUNDLÆGGENDE CYBERSIKKERHED OG FOREBYGGELSE AF TRUSLER (INTRODUKTION)

Cybersikkerhed beskytter netværk, systemer og data mod uautoriserede digitale angreb. Gode sikkerhedsvaner, opsatte firewalls, krav om flerfaktorgodkendelse og træning af medarbejdere i at genkende trusler er afgørende dele af virksomhedens forsvar.

LÆS HVERT KONTROLPUNKT GRUNDIGT, OG VÆLG ELLER SKRIV DET RIGTIGE SVAR.

Kontrolpunkt 1: Flervalgsopgave

1. Hvad er hovedformålet med et phishingangreb?

- A. At stjæle loginoplysninger og følsomme data
- B. At gøre et websted mere synligt i søgemaskiner
- C. At øge netværkets båndbredde
- D. At styre spejling mellem backupdatacentre

2. Hvilken mekanisme giver den stærkeste beskyttelse af konti?

- A. Flerfaktorgodkendelse med hardwarenøgler
- B. Komplekse adgangskoder, der skiftes hver 30. dag
- C. Login kun i arbejdstiden
- D. At skjule brugernavnet i offentlige kataloger

3. Hvad kendetegner en ransomwareinfektion?

- A. Kryptering af systemfiler og krav om betaling
- B. Skjult logning af tastetryk til fjerne servere
- C. Uautoriserede reklamer i browseren
- D. Brug af processoren til at udvinde kryptovaluta

4. Hvordan påvirker et zero-day-exploit forsvaret?

- A. Det rammer ukendte sårbarheder uden rettelser
- B. Det slår automatisk firmaets firewall fra
- C. Det tvinger systemet til en hård genstart
- D. Det koster intet at udbedre

5. Hvilken ramme styrer virksomheders sikkerhedskontroller?

- A. Retningslinjerne i NIST Cybersecurity Framework
- B. W3C's specifikationer for HTML5-dokumenter
- C. Installationsvejledninger til printerdrivere
- D. IETF's definitioner af routingprotokoller

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål tf 6

6. Phishing rammer kun private e-mailkonti.

○ Sandt ○ Falsk

7 Spørgsmål tf 7

7. Multifaktorgodkendelse (MFA) hjælper med at blokere credential stuffing-angreb.

○ Sandt ○ Falsk

8 Spørgsmål tf 8

8. Firewalls undersøger trafikken og blokerer uautoriseret adgang til porte.

○ Sandt ○ Falsk

9 Spørgsmål tf 9

9. Zero-day-exploits udbedres med almindelige opdateringer af antivirus.

○ Sandt ○ Falsk

10 Spørgsmål tf 10

10. En honeypot er en lokkeserver, der skal lokke cyberkriminelle.

○ Sandt ○ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

Læs hver sætning nedenfor, og udfyld det tomme felt med det rigtige ord fra ordbanken.

1. Netværksadministratorer installerer en _____ for at filtrere indgående trafik.
2. En angriber bruger en ukendt sårbarhed og et _____ til at omgå systemets rettelser.
3. Angribere sender forfalskede e-mails og driver _____ mod medarbejderne.
4. Ransomware er en ødelæggende form for _____ , der låser brugernes data.
5. God _____ for adgangskoder mindsker risikoen for tyveri af logins.
6. For at beskytte følsom kommunikation bruger man _____ protokoller.

ORDBANK MED FAGUDTRYK

BEREDSKAB EXPLOIT FIREWALL HYGIEJNE KRYPTERING LOKKEDUE MALWARE PHISHING

Skriv dine svar her:

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

Kontrolpunkt 4: Match sikkerhedsbegreber

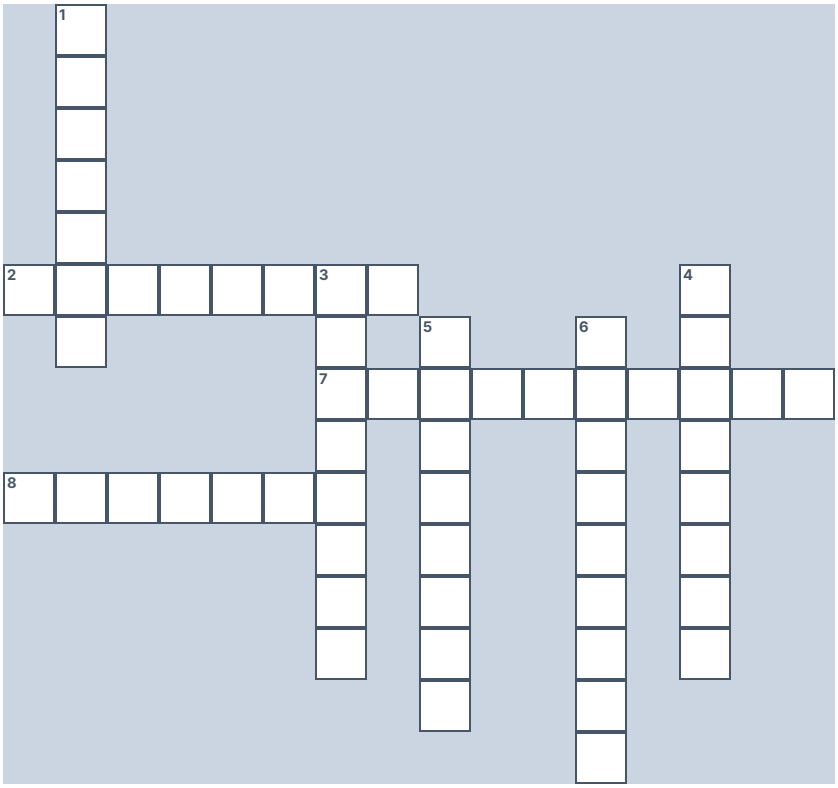
MATCH BEGREBER OG DEFINITIONER

Match hvert fagudtryk til venstre med den rigtige definition til højre ved at skrive det tilhørende bogstav (A-H) i indtastningsfeltet.

☐	1. Ransomwaretrussel	A	Faste retningslinjer som NIST til styring af cyberrisici.
☐	2. Flerfaktorgodkendelse	B	Fast plan for håndtering og begrænsning af sikkerhedsbrud.
☐	3. Zero-day-exploit	C	Barriere, der filtrerer trafikken efter sikkerhedsregler.
☐	4. Honeypot som lokkedue	D	Malware, der krypterer data og kræver betaling for at dekryptere dem.
☐	5. Firewall mod indtrængen	E	Udnyttelse af en sårbarhed, før leverandøren har udsendt en rettelse.
☐	6. Hændelsesberedskab	F	God praksis for håndtering af loginoplysninger og nøgler.
☐	7. Hygiejne for adgangskoder	G	Sikkerhedskontrol, der kræver to eller flere faktorer.
☐	8. Sikkerhedsramme	H	Lokkesystem, der skal lokke og analysere ondsindede aktører.

Kontrolpunkt 5: Kryds og tværs

Løs kryds og tværs ved at skrive bogstaver i de aktive hvide felter. Tallene svarer til nøglerne nedenfor.



VANDRETTE NØGLER

2. Barriere, der filtrerer indgående trafik efter faste sikkerhedsregler (8)

7. Beskyttelse, der gør følsom kommunikation ulæselig for andre (10)

8. Skadelig software, som ransomware er en ødelæggende form for (7)

LODRETTE NØGLER

1. Kode, der udnytter en sårbarhed, før der findes en rettelse (7)

3. Falsk server, en honeypot, der skal lokke og afsløre cyberkriminelle (8)

4. Forfalskede e-mails, der skal lokke medarbejdere til at afsløre logins (8)

5. God praksis for adgangskoder, der mindsker risikoen for tyveri (8)

6. Fast plan for at håndtere og begrænse sikkerhedsbrud (9)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

Brugere af skærmlæser og tastatur kan skrive krydsordssvarene direkte i tekstfelterne nedenfor.

VANDRETTE NØGLER

2 vandret: Barriere, der filtrerer indgående trafik efter faste sikkerhedsregler (8 bogstaver):

7 vandret: Beskyttelse, der gør følsom kommunikation ulæselig for andre (10 bogstaver):

8 vandret: Skadelig software, som ransomware er en ødelæggende form for (7 bogstaver):

LODRETTE NØGLER

1 lodret: Kode, der udnytter en sårbarhed, før der findes en rettelse (7 bogstaver):

3 lodret: Falsk server, en honeypot, der skal lokke og afsløre cyberkriminelle (8 bogstaver):

4 lodret: Forfalskede e-mails, der skal lokke medarbejdere til at afsløre logins (8 bogstaver):

5 lodret: God praksis for adgangskoder, der mindsker risikoen for tyveri (8 bogstaver):

6 lodret: Fast plan for at håndtere og begrænse sikkerhedsbrud (9 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

Find de 8 vigtige fagudtryk, der er skjult i gitteret nedenfor. Ordene kan stå vandret, lodret eller diagonalt.

W	U	V	F	M	K	B	H	A	B	C	Q	Æ	M	L
Æ	M	Æ	W	L	E	S	Y	O	K	L	E	J	O	O
L	E	S	R	H	O	O	G	S	T	O	U	W	V	H
B	R	C	U	S	Q	I	I	U	C	K	Y	E	V	Ø
A	A	X	C	Å	K	Y	E	G	L	K	I	Å	F	D
K	W	O	E	S	R	Z	J	R	C	E	W	B	I	A
S	L	Å	P	E	Y	M	N	P	A	D	E	Q	R	E
D	A	F	H	J	P	D	E	H	E	U	T	S	E	N
E	M	F	J	U	T	Å	U	I	X	E	G	S	W	Y
R	F	A	A	S	E	Q	O	S	P	R	W	Æ	A	S
E	L	T	W	U	R	D	O	H	L	Ø	B	G	L	U
B	Z	Z	K	A	I	T	Å	I	O	Ø	Ø	M	L	H
J	O	T	L	N	N	N	V	N	I	Q	I	S	S	H
Å	A	Q	X	G	G	X	C	G	T	Ø	T	Ø	B	I
N	Å	H	K	P	R	P	Z	C	N	Å	Ø	G	Æ	Q

ORDLISTE MED FAGUDTRYK

FIREWALL EXPLOIT PHISHING MALWARE HYGIEJNE KRYPTERING LOKKEDUE BEREDSKAB

Kontrolpunkt 6, alternativ: Tilgængelig ordmatchning

Match hvert af de 8 fagudtryk fra ordjagten med den rigtige definition ved at skrive bogstavet (A-H) i det tomme felt.

FAGUDTRYK
A. FIREWALL
B. EXPLOIT
C. PHISHING
D. MALWARE
E. HYGIEJNE
F. KRYPTERING
G. LOKKEDUE
H. BEREDSKAB

DEFINITIONER OG MATCHFELTER	
	1. God praksis for adgangskoder, der mindsker risikoen for tyveri.
	2. Beskyttelse, der gør følsom kommunikation ulæselig for andre.
	3. Barriere, der filtrerer indgående trafik efter faste sikkerhedsregler.
	4. Kode, der udnytter en sårbarhed, før der findes en rettelse.
	5. Falsk server, en honeypot, der skal lokke og afsløre cyberkriminelle.
	6. Fast plan for at håndtere og begrænse sikkerhedsbrud.
	7. Forfalskede e-mails, der skal lokke medarbejdere til at afsløre logins.
	8. Skadelig software, som ransomware er en ødelæggende form for.

Kontrolpunkt 7: Bogstavrod-udfordring

Sæt bogstaverne nedenfor i den rigtige rækkefølge, og find vigtige cybersikkerhedsbegreber. Skriv dine svar i indtastningsfelterne.

1. **LEWFAILR** _____

2. **SPGHNIHI** _____

3. **IYHEJENG** _____

4. **KUEDELOK** _____

5. **OTLPEIX** _____

6. **RLAMWEA** _____

7. **RPKREINGTY** _____

8. **BDABEESKR** _____

Bonusaktivitet: Tænk hurtigt

3 SVAR I HVER KATEGORI. DEN FØRSTE, DER UDFYLDER HELE LISTEN, VINDER.

1	Jobs inden for cybersikkerhed			
2	Grunde til at opdatere software			
3	Ting, en firewall kan blokere			
4	Advarselstegn i en e-mail			
5	Ting, du tager backup af			
6	Kendte typer af cyberangreb			
7	Ting, en honeypot kan lokke til sig			
8	Oplysninger, du aldrig bør dele			
9	Tegn på, at en computer er inficeret			
10	Film eller serier om hackere			
11	Sikkerhedslag, du kan bygge op			
12	Ting at øve i en sikkerhedsøvelse			
13	Sikkerhedsværktøjer, du kender			
14	Personer, du kan spørge om it-hjælp			
15	Ord, der begynder med 'cyber'			

Kontrolpunkt 8: Casestudier om cybersikkerhed

Anvend de begreber, du har lært, til at løse de virkelige scenarier nedenfor.

CASESTUDIE 1: GENOPRETNING EFTER RANSOMWARE



Scenarie: Et firmanetværk er ramt af ransomware, der låser vigtige databaser. Angriberne kræver 100.000 dollar i kryptovaluta. Firmaet har offline backups fra for 24 timer siden.

Diskussion: Analysér risikoen ved at betale, og vurdér planen for genopretning.

CASESTUDIE 2: FORSVAR MOD CREDENTIAL STUFFING



Scenarie: En onlinetjeneste rammes af credential stuffing, hvor hackere afprøver millioner af brugernavne og adgangskoder stjålet fra andre websteder.

Diskussion: Forklar, hvordan angrebet virker, og beskriv to forsvars-systemer.

Kontrolpunkt 9: Afkod chifferet

En cybersikkerhedsekspert beskytter netværkets aktiver mod trusselsaktører online. Brug bogstav-til-tal-nøglen nedenfor til at afkode beskeden ved at skrive de tilsvarende bogstaver i de tomme felter.

BOGSTAV-TIL-TAL-KRYPTERINGSNØGLE

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26 Æ=27 Ø=28 Å=29

13	6	1		19	20	15	16	16	5	18		4	5		6	12	5	19	20	5

1	14	7	18	5	2

Afkodet besked:

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z, 27 = Æ, 28 = Ø, 29 = Å).

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del A)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q1: Hvad er hovedformålet med cybersikkerhed?

At beskytte netværk, enheder og data mod uautoriseret adgang, angreb og utilsigtet skade.

Q2: Hvad er forskellen på phishing og spear phishing?

Phishing er brede kampagner mod tilfældige brugere, mens spear phishing rammer bestemte personer med personlige oplysninger.

Q3: Hvad er en firewall?

Et sikkerhedssystem, der overvåger og filtrerer trafik ind og ud efter faste regler.

Q4: Hvorfor er flerfaktorgodkendelse (MFA) nødvendig?

MFA tilføjer et vigtigt ekstra lag og forhindrer adgang, selv hvis angribere stjæler eller knækker adgangskoden.

Q5: Hvad kendetegner en computervirus?

Selvkopierende malware, der hæfter sig på rene filer og spreder sig, når den køres.

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del B)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q6: Hvordan låser ransomware data?

Den krypterer filerne med kryptografiske algoritmer, så de er ulæselige, indtil en nøgle bruges.

Q7: Hvad er en zero-day-sårbarhed?

En fejl i software, som leverandøren ikke kender, så der ikke er tid til at lave en rettelse, før den udnyttes.

Q8: Hvilken rolle spiller NIST-rammen?

Den giver frivillige retningslinjer og standarder, der hjælper organisationer med at styre og mindske cyberrisici.

Q9: Hvad er en plan for hændelsesberedskab?

Nedskrevne procedurer for at opdage, inddæmme og komme sig efter sikkerhedsbrud.

Q10: Hvordan udnytter social manipulation brugerne?

Psykologisk manipulation lokker medarbejdere til at afsløre adgangskoder eller hente skadelige filer.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del C)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og overholdelse af databeskyttelsesregler.

Q1: Hvordan overbelaster et DDoS-angreb servere?

Millioner af kaprede enheder i et botnet oversvømmer serveren med trafik, til båndbredde og processor er opbrugt.

Q2: Hvad er forskellen på symmetrisk og asymmetrisk kryptering?

Symmetrisk kryptering bruger én nøgle til begge dele, mens asymmetrisk bruger et par af en offentlig og en privat nøgle.

Q3: Hvordan udfører hackere SQL-injektion?

De skriver skadelige SQL-kommandoer i formularfelter og narrer databasen til at udlevere brugeroplysninger.

Q4: Hvad er lateral bevægelse ved indtrængen?

Angriberen bruger adgangen til én server til at kompromittere andre forbundne systemer på det interne netværk.

Q5: Hvordan omdirigerer DNS-forfalskning trafik?

Den ændrer navneserverens cache, så brugere sendes til skadelige kopier af de rigtige websteder.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del D)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og overholdelse af databeskyttelsesregler.

Q6: Hvad er en hardwarenøgle?

En fysisk enhed (som en YubiKey), der danner kryptografiske beviser og giver det stærkeste forsvar mod phishing.

Q7: Hvordan bruger sikkerhedsteams honeypots?

De opsætter lokkeservere uden for produktionen for at opdage indtrængen tidligt og analysere angribernes metoder.

Q8: Hvad er princippet om mindste rettigheder?

At brugere kun får de rettigheder, der er absolut nødvendige for deres arbejde.

Q9: Hvordan udnytter et man-in-the-middle-angreb forbindelser?

Angriberen opsnapper og ændrer kommunikationen mellem to enheder på ukrypterede net og stjæler sessionsnøgler og logins.

Q10: Hvad er tegn på kompromittering (IOC'er)?

Tekniske spor som usædvanlige ændringer i registreringsdatabasen eller mistænkelig trafik, der viser, at et system er brudt.

Del 11: 10 fakta og indsigter om cybersikkerhed fra virkeligheden

Gennemgå fakta om sikkerhedsbrud, forsvarsmekanismer og krav til overholdelse.

1. SIKKERHEDSINDSIGT

Angribere scanner konstant internettet for sårbare servere og sender phishing-mails til medarbejdernes indbakker.

2. SIKKERHEDSINDSIGT

Menneskelige fejl, fx klik på phishing-links, er en almindelig faktor i databrud, og derfor er træning vigtig.

3. SIKKERHEDSINDSIGT

Omkostninger ved databrud omfatter juridiske bøder, tab af kunder, efterforskning og reparation og kan løbe op i millioner af dollars.

4. SIKKERHEDSINDSIGT

Phishing-resistent multifaktorgodkendelse (MFA), fx hardwaresikkerhedsnøgler, er den stærkeste type MFA og den standard, CISA opfordrer til. [2]

5. SIKKERHEDSINDSIGT

Ransomware er fortsat en stor trussel mod virksomhedsnetværk, og CISA opfordrer til offline, krypterede backups som et centralt forsvar. [4]

6. SIKKERHEDSINDSIGT

NIST Cybersecurity Framework 2.0 (2024) har seks kernefunktioner: Govern, Identify, Protect, Detect, Respond, Recover. [1]

7. SIKKERHEDSINDSIGT

Bots til credential stuffing afprøver lækkede par af brugernavne og adgangskoder i stor skala mod login-portaler til netbanker og webbutikker.

8. SIKKERHEDSINDSIGT

Der findes markeder for zero-day-exploits verden over, hvor alvorlige sårbarheder kan sælges for store beløb, før de lukkes.

9. SIKKERHEDSINDSIGT

En honeypot slår straks alarm, fordi almindelige brugere ingen grund har til at tilgå den.

10. SIKKERHEDSINDSIGT

Transport Layer Security (TLS) krypterer browsersessioner og forhindrer aflytning på offentligt wi-fi.

Tekniske referencer og kilder

Studieguiden og de interaktive opgaver er sammensat ud fra globale standarder fra NIST, OWASP og regler om databeskyttelse.

VIDENSKABELIGE OG BRANCHEMÆSSIGE REFERENCER

[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

Facitliste: Kontrolpunkt 1 – Flervalg

1 **Phishingangreb** PHISHING — Rigtigt svar: A

UNDERVISNINGSNOTE

Phishingkampagner forsøger at stjæle loginoplysninger og følsomme data med forfalskede e-mails.

2 **Beskyttelse af konti** MFA-NØGLE — Rigtigt svar: A

UNDERVISNINGSNOTE

Flerfaktorgodkendelse (MFA) med hardwarenøgler giver det stærkeste forsvar af konti.

3 **Ransomwaretrussel** RANSOMWARE — Rigtigt svar: A

UNDERVISNINGSNOTE

Ransomware krypterer vigtige systemer og data og kræver kryptovaluta for nøglerne.

4 **Zero-day-sårbarhed** ZERO-DAY — Rigtigt svar: A

UNDERVISNINGSNOTE

Zero-day-trusler udnytter ukendte fejl, før leverandøren har en rettelse klar.

5 **Sikkerhedsrammer** RAMMER — Rigtigt svar: A

UNDERVISNINGSNOTE

Rammer som NIST giver faste retningslinjer til at styre og mindske cyberrisici.

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 **Mål for phishing** PHISHING — **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

Phishing rammer både firmanetværk og private konti for at få flere angrebsveje.

7 **Spørgsmål 7** — **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

MFA kræver en ekstra faktor, så en stjålet adgangskode alene er som regel ikke nok til at logge ind.

8 **Firewall for trafik** FIREWALL — **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

Firewalls undersøger og blokerer trafik på bestemte porte og frasorterer uautoriserede forbindelser.

9 **Reaktion på zero-day** ZERO-DAY — **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

Zero-day-fejl kræver koderettelser og WAF-filtrering, da der endnu ikke findes signaturer.

10 **Honeypots som lokkeduer** HONEYPOT — **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

Honeypots er lokkeservere, som sikkerhedsteams bruger til at lokke, advare om og studere angribere.

Ordfacit og bedømmelsesvejledning

Bedømmelsesvejledning til underviseren: Giv 1 point for hver korrekt matchning (8 point i alt) og hvert korrekt kontekstord (6 point i alt).

KONTROLPUNKT 4: FACIT TIL BEGREBSMATCHNING

D 1. Ransomwaretrussel	G 2. Flerfaktorgodkendelse	E 3. Zero-day-exploit	H 4. Honeypot som lokkedue
C 5. Firewall mod indtrængen	B 6. Hændelsesberedskab	F 7. Hygiejne for adgangskoder	A 8. Sikkerhedsramme

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 FIREWALL	2 EXPLOIT	3 PHISHING	4 MALWARE
5 HYGIEJNE	6 KRYPTERING		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 E – HYGIEJNE	2 F – KRYPTERING	3 A – FIREWALL	4 B – EXPLOIT
5 G – LOKKEDUE	6 H – BEREDSKAB	7 C – PHISHING	8 D – MALWARE

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare Ransomwaretrussel, Flerfaktorgodkendelse og Zero-day-exploit med egne ord og give et eksempel på hvert begreb.

Casestudier:
Bed eleverne begrunde deres anbefalinger med fakta fra opgavearket frem for antagelser.

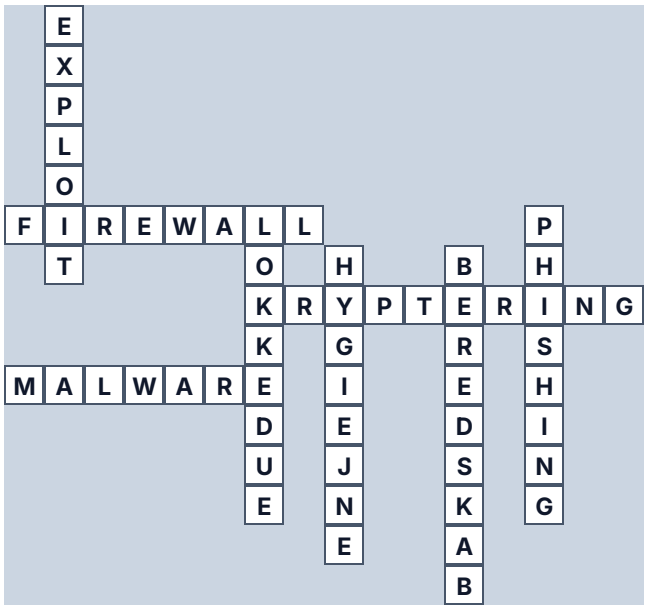
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

W	U	V	F	M	K	B	H	A	B	C	Q	Æ	M	L
Æ	M	Æ	W	L	E	S	Y	O	K	L	E	J	O	O
L	E	S	R	H	O	O	G	S	T	O	U	W	V	H
B	R	C	U	S	Q	I	I	U	C	K	Y	E	V	Ø
A	A	X	C	Å	K	Y	E	G	L	K	I	Å	F	D
K	W	O	E	S	R	Z	J	R	C	E	W	B	I	A
S	L	Å	P	E	Y	M	N	P	A	D	E	Q	R	E
D	A	F	H	J	P	D	E	H	E	U	T	S	E	N
E	M	F	J	U	T	Å	U	I	X	E	G	S	W	Y
R	F	A	A	S	E	Q	O	S	P	R	W	Æ	A	S
E	L	T	W	U	R	D	O	H	L	Ø	B	G	L	U
B	Z	Z	K	A	I	T	Å	I	O	Ø	Ø	M	L	H
J	O	T	L	N	N	N	V	N	I	Q	I	S	S	H
Å	A	Q	X	G	G	X	C	G	T	Ø	T	Ø	B	I
N	Å	H	K	P	R	P	Z	C	N	Å	Ø	G	Æ	Q

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

2 vandret: FIREWALL Barriere, der filtrerer indgående trafik efter faste sikkerhedsregler (8 bogstaver)

7 vandret: KRYPTERING Beskyttelse, der gør følsom kommunikation ulæselig for andre (10 bogstaver)

8 vandret: MALWARE Skadelig software, som ransomware er en ødelæggende form for (7 bogstaver)

LODRETTE NØGLER

1 lodret: EXPLOIT Kode, der udnytter en sårbarhed, før der findes en rettelse (7 bogstaver)

3 lodret: LOKKEDUE Falsk server, en honeypot, der skal lokke og afsløre cyberkriminelle (8 bogstaver)

4 lodret: PHISHING Forfalskede e-mails, der skal lokke medarbejdere til at afsløre logins (8 bogstaver)

5 lodret: HYGIEJNE God praksis for adgangskoder, der mindsker risikoen for tyveri (8 bogstaver)

6 lodret: BEREDSKAB Fast plan for at håndtere og begrænse sikkerhedsbrud (9 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1.	LEWFAILR	FIREWALL	5.	OTLPEIX	EXPLOIT
2.	SPGHNIHI	PHISHING	6.	RLAMWEA	MALWARE
3.	IYHEJENG	HYGIEJNE	7.	RPKREINGTY	KRYPTERING
4.	KUEDELOK	LOKKEDUE	8.	BDABEESKR	BEREDSKAB

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"MFA STOPPER DE FLESTE ANGREB"

Facit til casestudier

A Casestudie 1: Genopretning efter ransomware

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: Et firmanetværk er ramt af ransomware, der låser vigtige databaser. Angriberne kræver 100.000 dollar i kryptovaluta. Der findes offline backups fra for 24 timer siden.
- Anbefalet strategi og løsning: Risiko ved at betale: Betaling garanterer ikke dekryptering, gør firmaet til et mål og finansierer kriminalitet. Genopretning: Isolér de smittede maskiner, slet de kompromitterede servere, og gendan fra offline backups. Luk den oprindelige indgang (phishing eller exploit), så angrebet ikke gentager sig.

B Casestudie 2: Forsvar mod credential stuffing

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En onlinetjeneste rammes af credential stuffing, hvor hackere afprøver millioner af stjålne logins fra andre websteder.
- Anbefalet strategi og løsning: Mekanisme: Angribere udnytter genbrugte adgangskoder og logger ind med automatiske bots. Forsvar: 1. MFA blokerer login, selv når adgangskoden er rigtig. 2. Begrænsning af forsøg og CAPTCHA stopper bots i at bombardere loginsiderne.