Navn: _____ Dato: _____ Poeng: _____

Grunnleggende cybersikkerhet og trusler på nett Forebygging

Cybersikkerhetstrusler, nettverksbrannmurer, flerfaktorautentisering, sikkerhetsrammeverk

LÆRINGSOVERSIKT: GRUNNLEGGENDE CYBERSIKKERHET

SIKRET
DATAKRYPTERING
256-bits AES-standard

I SAMSVAR
GLOBALE STANDARDER
Rammeverk for GDPR og CCPA

ZERO TRUST
TILGANGSPOLICY
Flerfaktorautentisering

Velkommen! Dette aktivitetsheftet veileder deg gjennom de grunnleggende prinsippene i cybersikkerhet og forebygging av trusler på nettet. Du utforsker trusler fra skadevare, flerfaktorautentisering, nettverksbrannmurer og rammeverk for håndtering av hendelser.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk cybersikkerhet og forebygging av trusler.**
- [ ] **Del 5-7: Løs kryssord og ordsøk.**
- [ ] **Del 8-9: Løs casestudier og chifferutfordringen.**
- [ ] **Del 10: Gå gjennom sidene med grunnleggende og avanserte vanlige spørsmål.**
- [ ] **Del 11: Utforsk 10 interessante fakta fra virkeligheten.**
- [ ] **Bonus: Tenk raskt-utfordring.**

Åpne VPN.coms veiledning om cybersikkerhet

URL: https://www.vpn.com/no/cybersikkerhet/

Din læringsveiledning for grunnleggende cybersikkerhet

- Identifiser vanlige angrepsveier for skadevare, nettfisking og inntrenging i bedriftsnettverk.
- Innfør standard sikkerhetskontroller innen cybersikkerhet, blant annet MFA, brannmurer og endepunktsforsvar.
- Vurder prosedyrer for hendelseshåndtering for å redusere konsekvensene av datainnbrudd.
- Analyser organisatoriske risikofaktorer og sikkerhetstilpasning under NIST-retningslinjene.
- Konfigurer rutiner for sikkerhetshygiene for å motvirke automatisert credential stuffing.

INSTRUKSJONER FOR CYBERSIKKERHETSGUIDE

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på forebygging av trusler. Avslutt med bonusaktiviteten Tenk raskt.

GRUNNLEGGENDE CYBERSIKKERHET OG TRUSSELFOREBYGGING (INNLEDNING)

Cybersikkerhet beskytter nettverk, systemer og data mot uautoriserte digitale angrep. Å utvikle robuste sikkerhetsvaner, konfigurere brannmurer, kreve flerfaktorautentisering og lære opp ansatte i å gjenkjenne trusler er viktige deler av forsvaret av et bedriftsnettverk.

LES HVERT KONTROLLPUNKT NØYE OG VELG ELLER SKRIV DET RIKTIGE SVARET.

Kontrollpunkt 1: Flervalgsutfordring

1. Hva er hovedmålet med et phishing-angrep?

- A. Å stjele legitimasjon og sensitive brukerdata
- B. Å forbedre nettstedets synlighet i søkemotorer
- C. Å øke kapasiteten på nettverksbåndbredden
- D. Å styre replikering mellom sikkerhetskopidatasentre

2. Hvilken mekanisme gir sterkest kontobeskyttelse?

- A. Flerfaktorautentisering med maskinvarenøkler
- B. Komplekse passord som oppdateres hver trettiende dag
- C. Å begrense kontoinnlogging til arbeidstid
- D. Å skjule kontoens brukernavn fra offentlige kataloger

3. Hva kjennetegner nyttelasten i en løsepengevirus-infeksjon?

- A. Å kryptere systemfiler og kreve betaling
- B. Å logge tastetrykk i det skjulte til eksterne servere
- C. Å injisere uautorisert reklame i nettlesere
- D. Å bruke lokale CPU-ressurser til å utvinne kryptovaluta

4. Hvordan påvirker en zero-day-sårbarhet sikkerhetsforsvaret?

- A. Den retter seg mot uoppdaterte, ukjente sårbarheter
- B. Den deaktiverer automatisk bedriftens brannmur
- C. Den tvinger systemet til å utføre en hard omstart
- D. Den krever null budsjett å utbedre

5. Hvilket rammeverk styrer sikkerhetskontrollene i bedrifter?

- A. Retningslinjer fra NIST Cybersecurity Framework
- B. Spesifikasjoner for W3C HTML5-dokumentskjema
- C. Installasjonshåndbøker for skriverdrivere
- D. IETF-definisjoner av rutingprotokoller

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål (sant/usant) 6

6. Nettfiskingsangrep retter seg bare mot personlige e-postkontoer.

- ◯ Sant
- ◯ Usant

7 Spørsmål (sant/usant) 7

7. Flerfaktorautentisering bidrar til å blokkere angrep med gjenbruk av stjålne påloggingsopplysninger (credential stuffing).

- ◯ Sant
- ◯ Usant

8 Spørsmål (sant/usant) 8

8. Brannmurer inspiserer nettverkstrafikk for å blokkere uautorisert portadgang.

- ◯ Sant
- ◯ Usant

9 Spørsmål (sant/usant) 9

9. Utbedring av zero-day-utnyttelser krever vanlige oppdateringer av antivirusdefinisjoner.

- ◯ Sant
- ◯ Usant

10 Spørsmål (sant/usant) 10

10. En honeypot er en lokkeserver som brukes til å lokke til seg nettkriminelle.

- ◯ Sant
- ◯ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

Les hver setning nedenfor og fyll ut det tomme feltet med riktig begrep fra ordbanken.

1. Nettverksadministratorer installerer en _____ for å filtrere innkommende trafikk.

2. En angriper bruker en _____ for en nulldagssårbarhet for å omgå systemoppdateringer.

3. Angripere sender forfalskede e-poster for å gjennomføre kampanjer med _____ mot ansatte.

4. Løsepengevirus er en destruktiv form for _____ som låser brukerens data.

5. Å etablere god _____ reduserer risikoen for tyveri av legitimasjon.

6. For å beskytte sensitiv kommunikasjon bruker brukere _____ -protokoller.

ORDBANK

BRANNMUR EXPLOIT FLERFAKTOR KRYPTERING LØSEPENGEVIRUS NETTFISKING PASSORDHYGIENE SKADEVARE

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble sikkerhetsbegreper

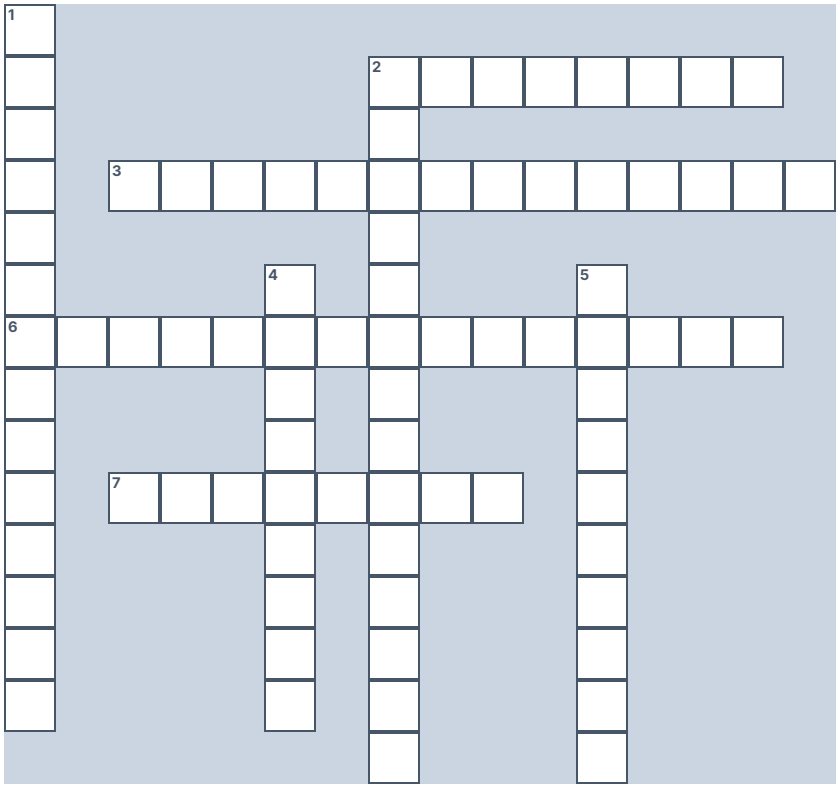
KOBLE DEFINISJONER

Koble hvert fagbegrep til venstre med riktig definisjon til høyre ved å skrive den tilhørende bokstaven (A-H) i det utfyllbare feltet.

☐	1. Løsepengevare-trussel	**A**	Strukturerte retningslinjer som NIST som brukes til å håndtere cyberrisiko.
☐	2. Flerfaktorautentisering	**B**	Strukturert plan for håndtering og begrensning av sikkerhetsbrudd.
☐	3. Zero-day-utnyttelse	**C**	Nettverksbarriere som filtrerer trafikk basert på sikkerhetsregler.
☐	4. Lokkedue (honeypot)	**D**	Skadevare som krypterer data og krever pengebetaling for dekryptering.
☐	5. Inntrengingsbrannmur	**E**	Utnyttelse av en sårbarhet som angripes før leverandøren har gitt ut en oppdatering.
☐	6. Hendelseshåndtering	**F**	Beste praksis for å håndtere legitimasjon og autentiseringsnøkler.
☐	7. Passordhygiene	**G**	Sikkerhetsvalidering som krever to eller flere autentiseringsfaktorer.
☐	8. Sikkerhetsrammeverk	**H**	Lokkesystem som settes opp for å lokke til seg og analysere ondsinnede aktører.

Kontrollpunkt 5: Kryssord

Løs kryssordet ved å skrive bokstaver i de aktive hvite rutene. Tallene tilsvarer hintene nedenfor.



VANNRETT

2. Nettverksbarriere som filtrerer trafikk etter sikkerhetsregler (8)

3. God praksis for å håndtere legitimasjon og autentiseringsnøkler (14)

6. Utnyttelse av en sårbarhet før leverandøren har gitt ut en oppdatering (15)

7. Lokkesystem som settes opp for å tiltrekke og analysere ondsinnede aktører (8)

LODDRETT

1. Skadevare som krypterer data og krever betaling for dekryptering (14)

2. Strukturert plan for å håndtere og dempe sikkerhetsbrudd (14)

4. Strukturerte retningslinjer, som NIST, brukt til å styre cyberrisiko (9)

5. Sikkerhetsvalidering som krever to eller flere autentiseringsfaktorer (10)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

Brukere av skjermleser og tastatur kan skrive inn kryssordsvarene direkte i tekstfeltene nedenfor.

VANNRETT

2 vannrett: Nettverksbarriere som filtrerer trafikk etter sikkerhetsregler (8 bokstaver):

3 vannrett: God praksis for å håndtere legitimasjon og autentiseringsnøkler (14 bokstaver):

6 vannrett: Utnyttelse av en sårbarhet før leverandøren har gitt ut en oppdatering (15 bokstaver):

7 vannrett: Lokkesystem som settes opp for å tiltrekke og analysere ondsinnede aktører (8 bokstaver):

LODDRETT

1 loddrett: Skadevare som krypterer data og krever betaling for dekryptering (14 bokstaver):

2 loddrett: Strukturert plan for å håndtere og dempe sikkerhetsbrudd (14 bokstaver):

4 loddrett: Strukturerte retningslinjer, som NIST, brukt til å styre cyberrisiko (9 bokstaver):

5 loddrett: Sikkerhetsvalidering som krever to eller flere autentiseringsfaktorer (10 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

Finn de 8 sentrale ordforrådsbegrepene som er skjult i rutenettet nedenfor. Ordene kan stå vannrett, loddrett eller diagonalt.

A G Q L P R D N O C D I J B B

E Q T N R U Y U W J L Ø N G Ø

N U H Æ Z M I L F T Ø W A P W

E L T E V N U L N R S M L O U

I I R L R N R D I Ø E Q P N Z

G X A P O A Ø A S S P B S A H

Y M M R T R O G B M E J P G O

H J M P K B Ø S C Å N Å A Ø N

D B E O A Y Æ E N D G F K Q E

R Z V R F S Æ X I E E Ø S C Y

O Z E N R F H P I Å V Z D D P

S Q R T E L Z L Æ T I M E Å O

S A K O L T Å O T N R H R U T

A Y G M F Z K I C Ø U D E C Ø

P Q X Å Q Å X T W B S I B Y R

ORDLISTE

LØSEPENGEVIRUS FLERFAKTOR NULLDAGSEXPLOIT HONEYPOT BRANNMUR

BEREDSKAPSPLAN PASSORDHYGIENE RAMMEVERK

Kontrollpunkt 6, alternativ: Tilgjengelig ordkobling

Koble hvert av de 8 fagbegrepene fra ordsøket til riktig definisjon ved å skrive bokstaven (A-H) i det tomme feltet.

BEGREPER
A. LØSEPENGEVIRUS
B. FLERFAKTOR
C. NULLDAGSEXPLOIT
D. HONEYPOT
E. BRANNMUR
F. BEREDSKAPSPLAN
G. PASSORDHYGIENE
H. RAMMEVERK

DEFINISJONER OG TILHØRENDE FELT	
	1. Nettverksbarriere som filtrerer trafikk etter sikkerhetsregler.
	2. Strukturert plan for å håndtere og dempe sikkerhetsbrudd.
	3. Skadevare som krypterer data og krever betaling for dekryptering.
	4. Sikkerhetsvalidering som krever to eller flere autentiseringsfaktorer.
	5. God praksis for å håndtere legitimasjon og autentiseringsnøkler.
	6. Strukturerte retningslinjer, som NIST, brukt til å styre cyberrisiko.
	7. Utnyttelse av en sårbarhet før leverandøren har gitt ut en oppdatering.
	8. Lokkesystem som settes opp for å tiltrekke og analysere ondsinnede aktører.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale begreper innen cybersikkerhet. Skriv svarene dine i svarboksene.

1. IEGVNSØERLU SPE
2. UAXGLSONTI LPLED
3. NRBNMRUA
4. ADNGSYREHE IPSO
5. TARLRKFFOE
6. OTEPHYON
7. PASBPERNSL AEKD
8. KERRMAVEM

Bonusaktivitet: Tenk raskt

3 SVAR PER KATEGORI. DEN SOM FYLLER UT LISTEN FØRST, VINNER.

1	Jobber innen cybersikkerhet			
2	Grunner til å oppdatere programvare			
3	Ting en brannmur kan blokkere			
4	Advarselstegn i en e-post			
5	Ting du tar sikkerhetskopi av			
6	Kjente typer nettangrep			
7	Ting en honningkrukke kan lokke til seg			
8	Informasjon du aldri bør dele			
9	Tegn på at en datamaskin er infisert			
10	Filmer eller serier om hackere			
11	Sikkerhetslag du kan bygge			
12	Ting å øve på i en sikkerhetsøvelse			
13	Sikkerhetsverktøy du kjenner til			
14	Personer du kan spørre om IT-hjelp			
15	Ord som begynner med «cyber»			

Kontrollpunkt 8: Casestudier om cybersikkerhet

Bruk begrepene du har lært til å løse de virkelige scenarioene nedenfor.

CASESTUDIE 1: STRATEGI FOR GJENOPPRETTING ETTER LØSEPENGEVIRUS



Scenario: Et bedriftsnettverk er infisert med løsepengevirus som låser kritiske databaser. Angriperne krever en utbetaling på $100,000 i kryptovaluta. Selskapet har offline-sikkerhetskopier fra for 24 timer siden.

Diskusjonsspørsmål: Analyser risikoene ved å betale, og vurder gjenopprettingsstrategien.

CASESTUDIE 2: FORSVAR MOT CREDENTIAL STUFFING



Scenario: En nettjeneste utsettes for et angrep med gjenbruk av stjålne påloggingsopplysninger (credential stuffing), der hackere tester millioner av brukernavn/passord-par som er stjålet fra andre nettsteder.

Diskusjonsspørsmål: Beskriv mekanismen bak dette angrepet, og skisser to forsvarssystemer.

Kontrollpunkt 9: Knekk chifferet

En cybersikkerhetsekspert beskytter nettverksressurser mot trusselaktører på nettet. Bruk nøkkelen med bokstaver og tall nedenfor til å dekryptere meldingen ved å skrive de tilhørende bokstavene i de tomme feltene.

NØKKEL FOR KRYPTERING AV BOKSTAV TIL TALL

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

2	18	21	11		6	12	5	18	6	1	11	20	15	18		6	15	18		29

19	9	11	18	5		19	25	19	20	5	13	5	20

Dekodet melding:

TIPS: HVERT TALL REPRESENTERER BOKSTAVENS PLASS I ALFABETET (F.EKS. 1 = A, 2 = B, 29 = Å).

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del A)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q1: Hva er hovedmålet med cybersikkerhet?

Hovedmålet er å beskytte nettverk, enheter og data mot uautorisert tilgang, angrep og utilsiktet skade.

Q2: Hvordan skiller nettfisking seg fra målrettet nettfisking (spear phishing)?

Nettfisking er en bred e-postkampanje mot tilfeldige brukere, mens målrettet nettfisking (spear phishing) retter seg mot bestemte personer ved hjelp av personlige data.

Q3: Hva er en nettverksbrannmur?

En brannmur er et nettverkssikkerhetssystem som overvåker og filtrerer innkommende og utgående trafikk basert på forhåndsdefinerte sikkerhetsregler.

Q4: Hvorfor er flerfaktorautentisering (MFA) nødvendig?

MFA gir et viktig ekstra forsvarslag og hindrer tilgang selv om angripere stjeler eller knekker de primære passordopplysningene.

Q5: Hva kjennetegner et datavirus?

Et virus er selvkopierende skadevare som fester seg til rene filer og sprer seg mellom systemer når det kjøres.

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del B)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q6: Hvordan låser løsepengevirus lokale data?

Løsepengevirus bruker kryptografiske algoritmer til å kryptere brukerfiler, slik at de blir uleselige til en dekrypteringsnøkkel brukes.

Q7: Hva er en zero-day-sårbarhet?

En zero-day er en sikkerhetsfeil i programvare som er ukjent for leverandøren, slik at det ikke er tid til å utvikle en oppdatering før feilen utnyttes.

Q8: Hvilken rolle spiller NIST-rammeverket?

NIST-rammeverket gir frivillige retningslinjer og standarder som hjelper organisasjoner med å håndtere og redusere cybersikkerhetsrisiko.

Q9: Hva er en beredskapsplan for sikkerhetshendelser?

Det er et dokumentert sett med prosedyrer for å oppdage, begrense og gjenopprette etter sikkerhetsbrudd og kompromittering av nettverk.

Q10: Hvordan utnytter sosial manipulering brukere?

Sosial manipulering bruker psykologisk påvirkning for å lure ansatte til å røpe passord eller laste ned skadelige filer.

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del C)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q1: Hvordan overbelaster et DDoS-angrep webservere?

Et DDoS-angrep koordinerer millioner av kompromitterte botnett-enheter for å oversvømme en server med trafikk og uttømme grensene for båndbredde og CPU.

Q2: Hva er forskjellen mellom symmetrisk og asymmetrisk kryptering?

Symmetrisk kryptering bruker én enkelt nøkkel til kryptering og dekryptering, mens asymmetrisk kryptering bruker et nøkkelpar med offentlig og privat nøkkel.

Q3: Hvordan utfører hackere SQL-injeksjonsangrep?

Angripere skriver inn ondsinnede SQL-kommandoer i skjemafelt og lurer databasen i bakenden til å frigi uautoriserte brukerposter.

Q4: Hva er lateral bevegelse i nettverksinntrengninger?

Det er teknikken der angripere utnytter første tilgang til en server til å kompromittere andre sammenkoblede systemer i det interne nettverket.

Q5: Hvordan omdirigerer DNS-spoofing nettrafikk?

DNS-forfalskning endrer bufrede oppføringer i navnetjenere og leder legitime brukere til skadelige etterligningsnettsteder i stedet for de egentlige domenene.

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del D)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q6: Hva er en maskinvaresikkerhetsnøkkel?

Det er en fysisk enhet (som en YubiKey) som genererer kryptografiske autentiseringsbevis og gir maksimalt forsvar mot nettfiske på avstand.

Q7: Hvordan bruker sikkerhetsteam lokkefugl-honeypots?

Team setter inn lokkeservere utenfor produksjon for å oppdage inntrengninger tidlig og analysere angrepsmønstrene til uautoriserte aktører.

Q8: Hva er prinsippet om minste privilegium (least privilege)?

Det er sikkerhetsstandarden om å begrense brukernes tilgangsrettigheter til det absolutt nødvendige minimum for å utføre arbeidsrollene sine.

Q9: Hvordan utnytter et mellommannsangrep (Man-in-the-Middle) tilkoblinger?

En angriper avskjærer og endrer kommunikasjon mellom to enheter på ukrypterte nettverk og stjeler øktkoder og legitimasjon.

Q10: Hva er indikatorer på kompromittering (IOC-er)?

IOC-er er kriminaltekniske spor, som uvanlige endringer i registeret eller uautorisert IP-trafikk, som viser at et system er brutt inn i.

Del 11: 10 fakta om cybersikkerhet fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om sikkerhetsbrudd, forsvarsmekanismer og samsvarsstandarder.

1. SIKKERHETSINNSIKT

Angripere skanner hele tiden internett etter sårbare servere og sender nettfiske-e-poster til ansattes innbokser.

2. SIKKERHETSINNSIKT

Menneskelige feil, som å klikke på nettfiskingslenker, er en vanlig faktor i datalekkasjer, og derfor er opplæring viktig.

3. SIKKERHETSINNSIKT

Kostnader ved et datainnbrudd omfatter juridiske bøter, tap av kunder, etterforskning og utbedring, og kan komme opp i millioner av dollar.

4. SIKKERHETSINNSIKT

Nettfiskingsresistent MFA, som fysiske sikkerhetsnøkler, er den sterkeste typen MFA og standarden som CISA oppfordrer til. [2]

5. SIKKERHETSINNSIKT

Løsepengevirus er fortsatt en stor trussel mot bedriftsnettverk, og CISA oppfordrer til frakoblede, krypterte sikkerhetskopier som et viktig forsvar. [4]

6. SIKKERHETSINNSIKT

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

7. SIKKERHETSINNSIKT

Credential stuffing-roboter tester lekkede par av brukernavn og passord i stor skala mot påloggingsportaler hos banker og nettbutikker.

8. SIKKERHETSINNSIKT

Det finnes markeder for zero-day-utnyttelser over hele verden, der svært alvorlige sårbarheter kan selges for store summer før de blir rettet.

9. SIKKERHETSINNSIKT

Et honeypot-lokkesystem rapporterer inntrengingsvarsler umiddelbart, siden legitime brukere ikke har noen grunn til å få tilgang til det.

10. SIKKERHETSINNSIKT

Transport Layer Security (TLS) krypterer nettleserøkter og hindrer pakkesnusing i offentlige Wi-Fi-nettverk.

Tekniske referanser og kilder

Studieveiledningen og de interaktive oppgavene er satt sammen fra globale standarder fra NIST og OWASP og standarder for etterlevelse av personvern.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[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

Fasit: Kontrollpunkt 1 – flervalg

1 **Nettfiskingsangrep** NETTFISKING — **Riktig svar: A**

MERKNAD TIL LÆREREN

Nettfiskingskampanjer forsøker å stjele påloggingsopplysninger og sensitive brukerdata ved hjelp av forfalskede e-poster.

2 **Kontobeskyttelse** MFA-NØKKEL — **Riktig svar: A**

MERKNAD TIL LÆREREN

Flerfaktorautentisering (MFA) med maskinvaretokener gir det sterkeste forsvaret for kontotilgang.

3 **Trussel fra løsepengevirus** LØSEPENGEVIRUS — **Riktig svar: A**

MERKNAD TIL LÆREREN

Løsepengevirus krypterer kritiske systemer og data og krever betaling i kryptovaluta for dekrypteringsnøklene.

4 **Zero-day-sårbarhet** ZERO-DAY — **Riktig svar: A**

MERKNAD TIL LÆREREN

Zero-day-trusler utnytter ukjente sikkerhetshull som ikke er rettet, før leverandøren har gjort en rettelse tilgjengelig.

5 **Sikkerhetsrammeverk** RAMMEVERK — **Riktig svar: A**

MERKNAD TIL LÆREREN

Rammeverk som NIST gir strukturerte retningslinjer som kan hjelpe organisasjoner med å håndtere og redusere cyberrisiko.

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Målrettet nettfisking** NETTFISKING — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Nettfiskingsangrep retter seg både mot bedriftsnettverk og personlige kontoer for å utvide angrepsflatene.

7 **Spørsmål 7** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

MFA krever en andre faktor, så et stjålet passord alene er vanligvis ikke nok til å logge inn.

8 **Trafikkbrannmur** BRANNMUR — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Brannmurer inspiserer og blokkerer trafikk på bestemte nettverksporter for å filtrere ut uautoriserte tilkoblinger.

9 **Respons på zero-day-sårbarheter** ZERO-DAY — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Utbedring av zero-day-sårbarheter krever kodeoppdateringer og WAF-filtrering, siden signaturer ikke finnes ennå.

10 **Lokkefugl-honeypots** HONNINGKRUKKE — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Honningkrukker er villedende servere som sikkerhetsteam bruker til å lokke til seg, varsle om og studere ondsinnede aktører.

Fasit for ordforråd og vurderingsmatrise

Rettemal for læreren: Gi 1 poeng for hver riktige kobling (totalt 8 poeng) og hvert kontekstbegrep (totalt 6 poeng).

KONTROLLPUNKT 4: FASIT – KOBLE BEGREPER

D 1. Løsepengevare-trussel	G 2. Flerfaktorautentisering	E 3. Zero-day-utnyttelse	H 4. Lokkedue (honeypot)
C 5. Inntrengingsbrannmur	B 6. Hendelseshåndtering	F 7. Passordhygiene	A 8. Sikkerhetsrammeverk

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 BRANNMUR	2 EXPLOIT	3 NETTFISKING	4 SKADEVARE
5 PASSORDHYGIENE	6 KRYPTERING		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 E – BRANNMUR	2 F – BEREDSKAPSPLAN	3 A – LØSEPENGEVIRUS	4 B – FLERFAKTOR
5 G – PASSORDHYGIENE	6 H – RAMMEVERK	7 C – NULLDAGSEXPLOIT	8 D – HONEYPOT

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare Løsepengevare-trussel, Flerfaktorautentisering og Zero-day-utnyttelse med egne ord og gi et eksempel på hvert.

Casestudier:
Be elevene begrunne anbefalingene sine med fakta fra arbeidsarket i stedet for antakelser.

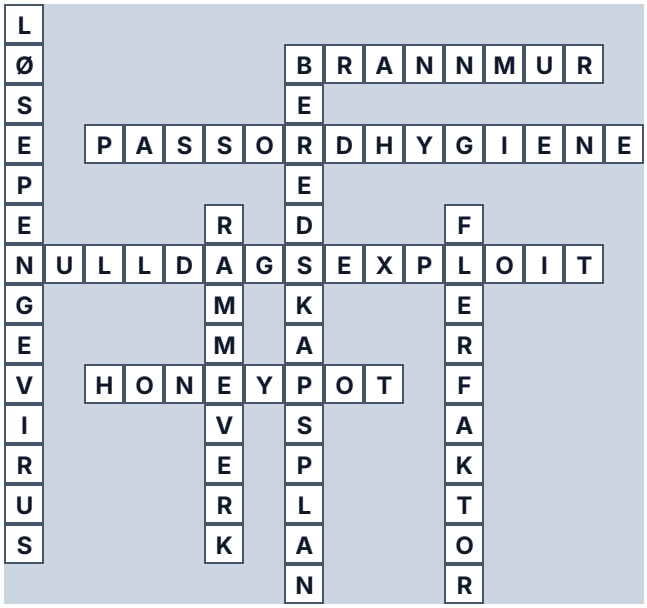
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

2 vannrett: BRANNMUR Nettverksbarriere som filtrerer trafikk etter sikkerhetsregler (8 bokstaver)

3 vannrett: PASSORDHYGIENE God praksis for å håndtere legitimasjon og autentiseringsnøkler (14 bokstaver)

6 vannrett: NULLDAGSEXPLOIT Utnyttelse av en sårbarhet før leverandøren har gitt ut en oppdatering (15 bokstaver)

7 vannrett: HONEYPOT Lokkesystem som settes opp for å tiltrekke og analysere ondsinnede aktører (8 bokstaver)

LODDRETT

1 loddrett: LØSEPENGEVIRUS Skadevare som krypterer data og krever betaling for dekryptering (14 bokstaver)

2 loddrett: BEREDSKAPSPLAN Strukturert plan for å håndtere og dempe sikkerhetsbrudd (14 bokstaver)

4 loddrett: RAMMEVERK Strukturerte retningslinjer, som NIST, brukt til å styre cyberrisiko (9 bokstaver)

5 loddrett: FLERFAKTOR Sikkerhetsvalidering som krever to eller flere autentiseringsfaktorer (10 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. IEGVNSØERLUSPE — **LØSEPENGEVIRUS**
2. UAXGLSONTILPLED — **NULLDAGSEXPLOIT**
3. NRBNMRUA — **BRANNMUR**
4. ADNGSYREHEIPSO — **PASSORDHYGIENE**
5. TARLRKFFOE — **FLERFAKTOR**
6. OTEPHYON — **HONEYPOT**
7. PASBPERNSLAEKD — **BEREDSKAPSPLAN**
8. KERRMAVEM — **RAMMEVERK**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"BRUK FLERFAKTOR FOR Å SIKRE SYSTEMET"

Fasit til casestudiene

A Casestudie 1: Strategi for gjenoppretting etter løsepengevirus

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: Et bedriftsnettverk er infisert med løsepengevirus som låser kritiske databaser. Angriperne krever en utbetaling på 100 000 dollar i kryptovaluta. Selskapet har frakoblede sikkerhetskopier fra 24 timer tilbake.
- Anbefalt strategi og løsning: Risiko ved å betale: Betaling garanterer ikke at filene blir dekryptert, merker selskapet som et mål som betaler, og finansierer kriminell virksomhet. Gjenopprettingsstrategi: Teamet bør isolere infiserte verter, slette kompromitterte servere og gjenopprette data fra frakoblede sikkerhetskopier. De må tette den første angrepsveien (phishing eller utnyttelse av sårbarhet) for å hindre umiddelbar ny infeksjon.

B Casestudie 2: Forsvar mot credential stuffing

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En nettjeneste opplever et credential stuffing-angrep der hackere tester millioner av brukernavn/passord-par stjålet fra andre nettsteder.
- Anbefalt strategi og løsning: Mekanisme: Angripere utnytter gjenbruk av passord på tvers av nettsteder og bruker automatiserte roboter til å logge inn på brukerkontoer. Forsvar: 1. Flerfaktorautentisering (MFA) blokkerer innloggingsforsøk selv om passordet er riktig. 2. Hastighetsbegrensning og CAPTCHA-er blokkerer automatisert robottrafikk som spammer innloggingsendepunkter.