Namn: _____ Datum: _____ Poäng: _____

Grunder i cybersäkerhet och hot på nätet Förebyggande

Cybersäkerhetshot, nätverksbrandväggar, multifaktorautentisering, säkerhetsramverk

LÄRÖVERSIKT: GRUNDER I CYBERSÄKERHET

SÄKRAD
DATAKRYPTERING
256-bitars AES-standard

EFTERLEVANDE
GLOBALA STANDARDER
Ramverken GDPR och CCPA

ZERO TRUST
ÅTKOMSTPOLICY
Multifaktorautentisering

Välkommen! Det här aktivitetshäftet guidar dig genom grundläggande principer för cybersäkerhet och förebyggande av hot på nätet. Du utforskar hot från skadlig kod, flerfaktorsautentisering, nätverksbrandväggar och ramverk för incidenthantering.

KONTROLLPUNKTER I ARBETSBLADET

- [ ] **Del 1-4: Behärska cybersäkerhet och hothantering.**
- [ ] **Del 5-7: Lös korsord och ordsökare.**
- [ ] **Del 8-9: Lös fallstudier och chifferutmaning.**
- [ ] **Del 10: Gå igenom sidorna med grundläggande och avancerade vanliga frågor.**
- [ ] **Del 11: Utforska 10 intressanta fakta från verkligheten.**
- [ ] **Bonus: utmaningen Tänk snabbt.**

Öppna VPN.com:s guide om cybersäkerhet

URL: https://www.vpn.com/sv/cybersakerhet/

Din inlärningsplan för grunderna i cybersäkerhet

- Identifiera vanliga vektorer för skadlig kod, nätfiske och intrång i företagsnätverk.
- Inför vanliga cybersäkerhetskontroller, inklusive MFA, brandväggar och slutpunktsskydd.
- Utvärdera förfaranden för incidenthantering för att mildra effekterna av dataintrång.
- Analysera organisatoriska riskfaktorer och säkerhetsanpassning enligt NIST:s riktlinjer.
- Konfigurera säkerhetsrutiner för att motverka automatiserad credential stuffing.

ANVISNINGAR FÖR CYBERSÄKERHETSGUIDE

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om hotförebyggande. Avsluta med bonusaktiviteten Tänk snabbt.

GRUNDER I CYBERSÄKERHET OCH HOTFÖREBYGGANDE (INLEDNING)

Cybersäkerhet skyddar nätverk, system och data mot obehöriga digitala attacker. Att utveckla robusta säkerhetsvanor, konfigurera brandväggar, kräva multifaktorautentisering och utbilda personal i att känna igen hot är viktiga delar av försvaret av företagsnätverk.

LÄS VARJE KONTROLLPUNKT NOGGRANT OCH VÄLJ ELLER SKRIV DET RÄTTA SVARET.

Kontrollpunkt 1: Utmaning med flerval

1. Vad är det främsta målet med en nätfiskeattack?

- A. Att stjäla inloggningsuppgifter och känsliga användardata
- B. Att förbättra webbplatsens synlighet i sökmotorer
- C. Att öka nätverkets bandbreddskapacitet
- D. Att hantera replikering av datacenter för säkerhetskopior

2. Vilken mekanism ger det starkaste kontoskyddet?

- A. Flerfaktorsautentisering med hårdvarunycklar
- B. Komplexa lösenord som uppdateras var trettionde dag
- C. Att begränsa kontoinloggning till kontorstid
- D. Att dölja kontots användarnamn från offentliga kataloger

3. Vad kännetecknar nyttolasten i en infektion med utpressningsvirus?

- A. Kryptering av systemfiler och krav på betalning
- B. Att i tysthet logga tangenttryckningar till fjärrservrar
- C. Att injicera obehörig reklam i webbläsare
- D. Att använda lokala CPU-resurser för att utvinna kryptovaluta

4. Hur påverkar en zero day-sårbarhet säkerhetsförsvaret?

- A. Den riktar in sig på ej korrigerade, okända sårbarheter
- B. Den inaktiverar automatiskt företagets brandvägg
- C. Den tvingar systemet att göra en hård omstart
- D. Den kräver ingen budget för att åtgärdas

5. Vilket ramverk styr säkerhetskontroller i företag?

- A. Riktlinjerna i NIST Cybersecurity Framework
- B. W3C:s specifikationer för HTML5-dokumentscheman
- C. Manualer för installation av skrivardrivrutiner
- D. IETF:s definitioner av routingprotokoll

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga sant/falskt 6

6. Nätfiskeattacker riktas bara mot privata e-postkonton.

○ Sant ○ Falskt

7 Fråga sant/falskt 7

7. Multifaktorautentisering hjälper till att blockera credential stuffing-attacker.

○ Sant ○ Falskt

8 Fråga sant/falskt 8

8. Brandväggar granskar nätverkstrafik för att blockera obehörig åtkomst till portar.

○ Sant ○ Falskt

9 Fråga sant/falskt 9

9. Åtgärdande av zero day-sårbarheter kräver vanliga uppdateringar av antivirusdefinitioner.

○ Sant ○ Falskt

10 Fråga sant/falskt 10

10. En honeypot är en lockbetesserver som används för att locka till sig cyberbrottslingar.

○ Sant ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

Läs varje mening nedan och fyll i luckan med rätt term från ordbanken.

1. Nätverksadministratörer installerar en _____ för att filtrera inkommande trafik.
2. En angripare använder en nolldags- _____ för att kringgå systemuppdateringar.
3. Angripare skickar förfalskade e-postmeddelanden för att genomföra kampanjer med _____ mot anställda.
4. Ransomware är en destruktiv form av _____ som låser användarens data.
5. Starkt lösenords- _____ minskar risken för stöld av inloggningsuppgifter.
6. För att skydda känslig kommunikation använder användare protokoll för _____ .

ORDBANK

BRANDVÄGG EXPLOIT FLERFAKTOR HYGIEN INCIDENTPLAN KRYPTERING NÄTFISKE SKADLIG KOD

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av säkerhetsbegrepp

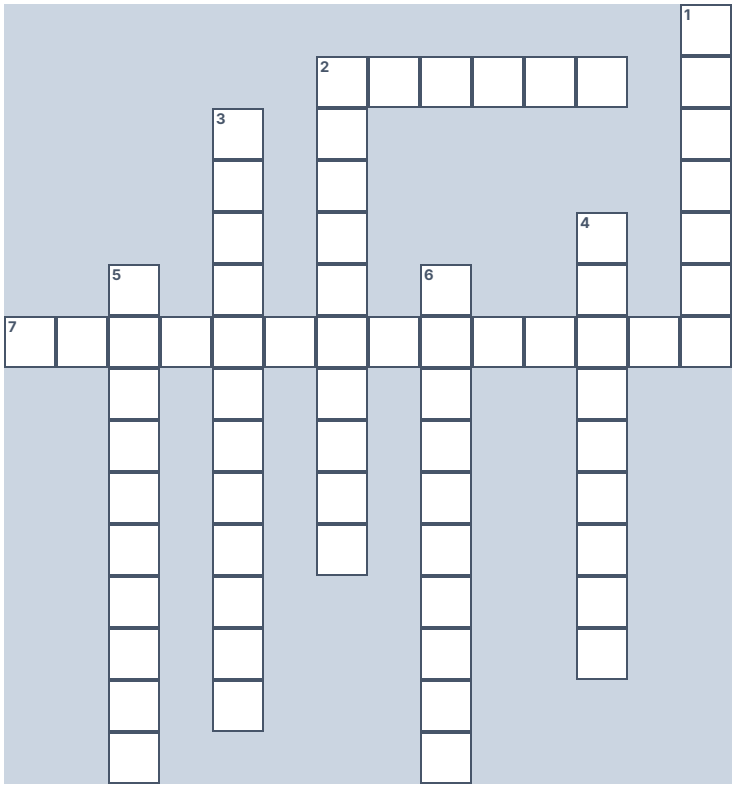
MATCHNING AV DEFINITIONER

Para ihop varje begrepp till vänster med rätt definition till höger genom att skriva motsvarande bokstav (A–H) i det ifyllbara fältet.

☐	1. Hot från ransomware	**A**	Strukturerade riktlinjer som NIST används för att hantera cyberrisker.
☐	2. Flerfaktorsautentisering	**B**	Strukturerad plan för att hantera och begränsa säkerhetsincidenter.
☐	3. Zero-day-sårbarhet	**C**	Nätverksbarriär som filtrerar trafik utifrån säkerhetsregler.
☐	4. Lockbete som honeypot	**D**	Skadlig kod som krypterar data och kräver betalning för dekryptering.
☐	5. Intrångsbrandvägg	**E**	Utnyttjande av en sårbarhet innan tillverkaren har släppt en korrigering.
☐	6. Incidenthantering	**F**	Bästa praxis för hantering av inloggningsuppgifter och autentiseringsnycklar.
☐	7. Lösenordshygien	**G**	Säkerhetsvalidering som kräver två eller flera autentiseringsfaktorer.
☐	8. Säkerhetsramverk	**H**	Lockbetessystem som sätts upp för att locka till sig och analysera illasinnade aktörer.

Kontrollpunkt 5: Korsord

Lös korsordet genom att skriva bokstäver i de aktiva vita rutorna. Siffrorna motsvarar ledtrådarna nedan.



VÅGRÄTT

2. Bästa praxis för att hantera inloggningsuppgifter och autentiseringsnycklar (6)

7. Utnyttjande av en sårbarhet innan tillverkaren har släppt en korrigering (14)

LODRÄTT

1. Strukturerade riktlinjer, som NIST, som används för att hantera cyberrisker (7)

2. Lockbetessystem som sätts upp för att locka och analysera illasinnade aktörer (10)

3. Strukturerad plan för att hantera och begränsa säkerhetsintrång (12)

4. Nätverksbarriär som filtrerar trafik utifrån säkerhetsregler (9)

5. Säkerhetsvalidering som kräver två eller fler autentiseringsfaktorer (10)

6. Skadlig kod som krypterar data och kräver betalning för dekryptering (10)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

Användare av skärmläsare och tangentbord kan skriva korsordssvaren direkt i textfälten nedan.

VÅGRÄTT

2 vågrätt: Bästa praxis för att hantera inloggningsuppgifter och autentiseringsnycklar (6 bokstäver):

7 vågrätt: Utnyttjande av en sårbarhet innan tillverkaren har släppt en korrigering (14 bokstäver):

LODRÄTT

1 lodrätt: Strukturerade riktlinjer, som NIST, som används för att hantera cyberrisker (7 bokstäver):

2 lodrätt: Lockbetessystem som sätts upp för att locka och analysera illasinnade aktörer (10 bokstäver):

3 lodrätt: Strukturerad plan för att hantera och begränsa säkerhetsintrång (12 bokstäver):

4 lodrätt: Nätverksbarriär som filtrerar trafik utifrån säkerhetsregler (9 bokstäver):

5 lodrätt: Säkerhetsvalidering som kräver två eller fler autentiseringsfaktorer (10 bokstäver):

6 lodrätt: Skadlig kod som krypterar data och kräver betalning för dekryptering (10 bokstäver):

Kontrollpunkt 6: Dolt ordsök

Hitta de 8 viktiga ordförrådstermerna som är gömda i rutnätet nedan. Orden kan vara vågräta, lodräta eller diagonala.

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

ORDLISTA

RANSOMWARE FLERFAKTOR NOLLDAGSATTACK HONUNGSFAT BRANDVÄGG
INCIDENTPLAN HYGIEN RAMVERK

Kontrollpunkt 6, alternativ: Tillgänglig matchning av ordförråd

Para ihop var och en av de 8 begreppen från ordsökningen med rätt definition genom att skriva bokstaven (A–H) på den tomma raden.

ORDLISTA

- **A. RANSOMWARE**
- **B. FLERFAKTOR**
- **C. NOLLDAGSATTACK**
- **D. HONUNGSFAT**
- **E. BRANDVÄGG**
- **F. INCIDENTPLAN**
- **G. HYGIEN**
- **H. RAMVERK**

DEFINITIONER OCH MATCHNINGSFÄLT

1. Nätverksbarriär som filtrerar trafik utifrån säkerhetsregler.
2. Strukturerad plan för att hantera och begränsa säkerhetsintrång.
3. Skadlig kod som krypterar data och kräver betalning för dekryptering.
4. Säkerhetsvalidering som kräver två eller fler autentiseringsfaktorer.
5. Bästa praxis för att hantera inloggningsuppgifter och autentiseringsnycklar.
6. Strukturerade riktlinjer, som NIST, som används för att hantera cyberrisker.
7. Utnyttjande av en sårbarhet innan tillverkaren har släppt en korrigering.
8. Lockbetessystem som sätts upp för att locka och analysera illasinnade aktörer.

Kontrollpunkt 7: Utmaning med blandade ord

Avkoda bokstäverna nedan för att avslöja viktiga begrepp och termer inom cybersäkerhet. Skriv dina svar i rutorna.

1. RWMOARAESN
2. DOALGCNASK TTAL
3. BVDRÄGNGA
4. NIGEHY
5. TARLRKFFOE
6. ANUSFHOGTN
7. TPDINNNLACE I
8. AVKRREM

Bonusaktivitet: Tänk snabbt

3 SVAR PER KATEGORI. DEN SOM FÖRST FYLLER I LISTAN VINNER.

1	Jobb inom cybersäkerhet			
2	Skäl till att uppdatera programvara			
3	Saker som en brandvägg kan blockera			
4	Varningstecken i ett e-postmeddelande			
5	Saker du säkerhetskopierar			
6	Välkända typer av cyberattacker			
7	Saker som en honeypot kan locka till sig			
8	Information du aldrig bör dela			
9	Tecken på att en dator är infekterad			
10	Filmer eller serier om hackare			
11	Säkerhetslager du kan bygga upp			
12	Saker att öva på i en säkerhetsövning			
13	Säkerhetsverktyg du känner till			
14	Personer du kan fråga om IT-hjälp			
15	Ord som börjar med "cyber"			

Kontrollpunkt 8: Fallstudier om cybersäkerhet

Tillämpa de begrepp du har lärt dig för att lösa de verkliga scenarierna nedan.

FALLSTUDIE 1: ÅTERHÄMTNINGSSTRATEGI EFTER RANSOMWARE



Scenario: Ett företagsnätverk har infekterats av utpressningsprogram som låser kritiska databaser. Angriparna kräver en betalning på 100 000 USD i kryptovaluta. Företaget har offlinebackuper från 24 timmar tillbaka.

Diskussionsfråga: Analysera riskerna med att betala och utvärdera återställningsstrategin.

FALLSTUDIE 2: FÖRSVAR MOT CREDENTIAL STUFFING



Scenario: En onlinetjänst utsätts för en credential stuffing-attack där hackare testar miljontals kombinationer av användarnamn och lösenord som stulits från andra webbplatser.

Diskussionsfråga: Beskriv hur den här attacken fungerar och redogör för två försvarssystem.

Kontrollpunkt 9: Knäck chiffret

En cybersäkerhetsexpert skyddar nätverkstillgångar mot hotaktörer online. Använd bokstav-till-siffra-nyckeln nedan för att avkoda meddelandet genom att skriva de matchande bokstäverna på de tomma raderna.

KRYPTERINGSNYCKEL FÖR BOKSTAV TILL SIFFRA

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 Å=27 Ä=28 Ö=29

19	11	25	4	4	1		19	25	19	20	5	13	5	20		13	5	4

6	12	5	18	1		6	1	11	20	15	18	5	18

Avkodat meddelande:

TIPS: VARJE SIFFRA MOTSVARAR BOKSTAVENS PLATS I ALFABETET (T.EX. 1 = A, 2 = B, 29 = Ö).

Kontrollpunkt 10: Grundläggande vanliga frågor om cybersäkerhet (Del A)

Gå igenom vanliga frågor och svar om att begränsa hot på nätet.

Q1: Vad är det huvudsakliga målet med cybersäkerhet?

Huvudmålet är att skydda nätverk, enheter och data mot obehörig åtkomst, attacker och oavsiktliga skador.

Q2: Hur skiljer sig nätfiske från spear phishing?

Nätfiske är en bred e-postkampanj som riktas mot slumpmässiga användare, medan spear phishing riktas mot specifika personer med hjälp av personliga uppgifter.

Q3: Vad är en nätverksbrandvägg?

En brandvägg är ett nätverkssäkerhetssystem som övervakar och filtrerar inkommande och utgående trafik utifrån fördefinierade säkerhetsregler.

Q4: Varför är flerfaktorsautentisering (MFA) nödvändig?

MFA lägger till ett viktigt försvarslager och förhindrar åtkomst även om angripare stjäl eller knäcker det primära lösenordet.

Q5: Vad kännetecknar ett datorvirus?

Ett virus är självreplikerande skadlig kod som fäster sig vid rena filer och sprids över system när den körs.

Kontrollpunkt 10: Grundläggande vanliga frågor om cybersäkerhet (Del B)

Gå igenom vanliga frågor och svar om att begränsa hot på nätet.

Q6: Hur låser ransomware lokala data?

Ransomware använder kryptografiska algoritmer för att kryptera användarnas filer så att de blir oläsliga tills en dekrypteringsnyckel tillämpas.

Q7: Vad är en zero-day-sårbarhet?

En zero day är en säkerhetslucka i programvara som är okänd för leverantören, så det finns ingen tid att ta fram en korrigering före utnyttjandet.

Q8: Vilken roll har NIST-ramverket?

NIST-ramverket innehåller frivilliga riktlinjer och standarder som hjälper organisationer att hantera och minska cybersäkerhetsrisker.

Q9: Vad är en incidenthanteringsplan för säkerhet?

Det är en dokumenterad uppsättning rutiner för att upptäcka, begränsa och återhämta sig från säkerhetsintrång och nätverkskompromisser.

Q10: Hur utnyttjar social manipulation användare?

Social manipulation använder psykologisk påverkan för att lura anställda att avslöja lösenord eller ladda ned skadliga filer.

Kontrollpunkt 10: Avancerade vanliga frågor om säkerhet (Del C)

Utforska avancerade tekniska aspekter av säkerhetsramverk, analys av skadlig kod och dataefterlevnad.

Q1: Hur överbelastar en DDoS-attack webbservrar?

En DDoS-attack samordnar miljontals komprometterade botnet-enheter för att översvämma en server med trafik och därmed uttömma bandbredd och CPU-gränser.

Q2: Vad är skillnaden mellan symmetrisk och asymmetrisk kryptering?

Symmetrisk kryptering använder en enda nyckel för kryptering och dekryptering, medan asymmetrisk kryptering använder ett nyckelpar med publik och privat nyckel.

Q3: Hur utför hackare SQL-injektionsattacker?

Angripare skriver in skadliga SQL-kommandon i formulärfält och lurar backend-databasen att lämna ut obehöriga användarposter.

Q4: Vad är lateral rörelse vid nätverksintrång?

Det är tekniken där angripare utnyttjar första åtkomsten till en server för att kompromettera andra sammankopplade system i det interna nätverket.

Q5: Hur omdirigerar DNS-förfalskning webbtrafik?

DNS-förfalskning ändrar cachade poster i namnservrar och leder legitima användare till skadliga webbplatser som liknar måldomänerna.

Kontrollpunkt 10: Avancerade vanliga frågor om säkerhet (Del D)

Utforska avancerade tekniska aspekter av säkerhetsramverk, analys av skadlig kod och dataefterlevnad.

Q6: Vad är en säkerhetsnyckel i hårdvara?

Det är en fysisk enhet (som en YubiKey) som genererar kryptografiska autentiseringsbevis och ger maximalt försvar mot nätfiske på distans.

Q7: Hur använder säkerhetsteam lockbetessystem (honeypots)?

Team driftsätter lockservrar utanför produktion för att upptäcka intrång tidigt och analysera attackmönstren hos obehöriga aktörer.

Q8: Vad är principen om minsta möjliga behörighet?

Det är säkerhetsstandarden att begränsa användarnas åtkomsträttigheter till det absolut minsta som krävs för deras arbetsroller.

Q9: Hur utnyttjar en man-in-the-middle-attack anslutningar?

En angripare fångar upp och ändrar kommunikation mellan två enheter i okrypterade nätverk och stjäl sessionstokens och inloggningsuppgifter.

Q10: Vad är indikatorer på intrång (IOC)?

IOC:er är kriminaltekniska ledtrådar, som ovanliga registerändringar eller skurktrafik från okända IP-adresser, som visar att ett system har utsatts för intrång.

Del 11: 10 verkliga fakta och insikter om cybersäkerhet

Gå igenom verkliga fakta om säkerhetsintrång, försvarsmekanismer och efterlevnadsstandarder.

1. SÄKERHETSINSIKT

Angripare skannar ständigt internet efter sårbara servrar och skickar nätfiskemejl till de anställdas inkorgar.

2. SÄKERHETSINSIKT

Mänskliga misstag, som att klicka på nätfiskelänkar, är en vanlig faktor vid dataintrång, vilket är anledningen till att utbildning är viktig.

3. SÄKERHETSINSIKT

Kostnader vid dataintrång omfattar juridiska böter, kundbortfall samt utredning och reparation, och kan uppgå till miljontals dollar.

4. SÄKERHETSINSIKT

Nätfiskeresistent MFA, till exempel fysiska säkerhetsnycklar, är den starkaste typen av MFA och den standard som CISA förespråkar. [2]

5. SÄKERHETSINSIKT

Ransomware är fortfarande ett stort hot mot företagsnätverk, och CISA förespråkar krypterade säkerhetskopior offline som ett viktigt försvar. [4]

6. SÄKERHETSINSIKT

NIST Cybersecurity Framework 2.0 (2024) har sex kärnfunktioner: Styra, Identifiera, Skydda, Upptäcka, Reagera, Återhämta. [1]

7. SÄKERHETSINSIKT

Credential stuffing-botar testar läckta kombinationer av användarnamn och lösenord i stor skala mot inloggningsportaler för bank och e-handel.

8. SÄKERHETSINSIKT

Marknader för nolldagsexploateringar finns över hela världen, där allvarliga sårbarheter kan säljas för stora summor innan de åtgärdas.

9. SÄKERHETSINSIKT

Ett honungsburksystem (honeypot) rapporterar intrångslarm omedelbart, eftersom legitima användare inte har någon anledning att komma åt det.

10. SÄKERHETSINSIKT

Transport Layer Security (TLS) krypterar webbläsarsessioner och förhindrar paketsniffning i publika Wi-Fi-nätverk.

Tekniska referenser och källor

Studieguiden och de interaktiva pusslen är sammanställda utifrån globala standarder från NIST och OWASP samt standarder för efterlevnad av dataskydd.

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[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

Facit: Kontrollpunkt 1 – Flerval

1 **Nätfiskeattacker** NÄTFISKE — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Nätfiskekampanjer försöker stjäla inloggningsuppgifter och känsliga användardata med förfalskade e-postmeddelanden. Källa: OWASP Secure Configuration.

2 **Kontoskydd** MFA-NYCKEL — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Multifaktorautentisering (MFA) med säkerhetsnycklar ger det starkaste försvaret av kontoåtkomst. Källa: NIST Digital Identity.

3 **Ransomware-hot** RANSOMWARE — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Ransomware krypterar kritiska system och data och kräver betalning i kryptovaluta för dekrypteringsnycklarna. Källa: Center for Internet Security (CIS).

4 **Nolldagarssårbarhet** NOLLDAGARS — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Nolldagshot utnyttjar oåtgärdade, okända säkerhetsbrister innan en korrigering från tillverkaren finns tillgänglig. Källhänvisning: OWASP Secure Configuration.

5 **Säkerhetsramverk** RAMVERK — Rätt svar: A

ANTECKNING FÖR LÄRAREN

Ramverk som NIST ger strukturerade riktlinjer som hjälper organisationer att hantera och minska cyberrisker. Källa: NIST Digital Identity.

Facit: Kontrollpunkt 2 – Sant eller falskt

6 **Riktat nätfiske** NÄTFISKE — Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Nätfiskeattacker riktas mot både företagsnätverk och privata konton för att utöka angreppsvägarna. Källa: OWASP Secure Configuration.

7 **Fråga 7** — Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

MFA kräver en andra faktor, så ett stulet lösenord räcker oftast inte för att logga in.

8 **Trafikbrandvägg** BRANDVÄGG — Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Brandväggar granskar och blockerar trafik på särskilda nätverksportar för att filtrera bort obehöriga anslutningar. Källa: Center for Internet Security (CIS).

9 **Åtgärder vid nolldagarshot** NOLLDAGARS — Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Att åtgärda zero day-sårbarheter kräver kodkorrigeringar och WAF-filtrering, eftersom signaturer ännu inte finns. Källa: OWASP Secure Configuration.

10 **Lockbetes-honeypots** HONEYPOT — Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Honeypots är vilseledande servrar som säkerhetsteam använder för att locka, varna och studera illasinnade aktörer. Källa: Center for Internet Security (CIS).

Facit för ordförråd och bedömningsmall

Bedömningsmatris för läraren: Ge 1 poäng för varje korrekt matchning (totalt 8 poäng) och kontextbegrepp (totalt 6 poäng).

KONTROLLPUNKT 4: FACIT – MATCHNING AV BEGREPP

D 1. Hot från ransomware	G 2. Flerfaktorsautentisering	E 3. Zero-day-sårbarhet	H 4. Lockbete som honeypot
C 5. Intrångsbrandvägg	B 6. Incidenthantering	F 7. Lösenordshygien	A 8. Säkerhetsramverk

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 BRANDVÄGG	2 EXPLOIT	3 NÄTFISKE	4 SKADLIG KOD
5 HYGIEN	6 KRYPTERING		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 E – BRANDVÄGG	2 F – INCIDENTPLAN	3 A – RANSOMWARE	4 B – FLERFAKTOR
5 G – HYGIEN	6 H – RAMVERK	7 C – NOLLDAGSATTACK	8 D – HONUNGSFAT

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara Hot från ransomware, Flerfaktorsautentisering och Zero-day-sårbarhet med egna ord och ge ett exempel på varje.

Fallstudier:
Be eleverna att stödja sina rekommendationer med fakta från arbetsbladet, inte med antaganden.

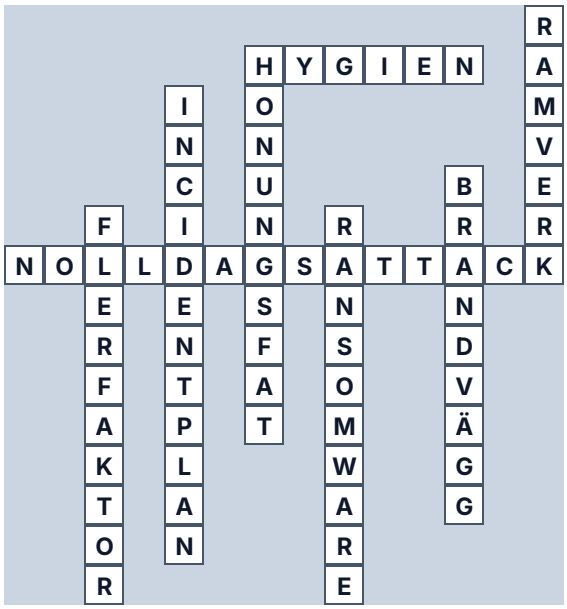
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

2 vågrätt: HYGIEN Bästa praxis för att hantera inloggningsuppgifter och autentiseringsnycklar (6 bokstäver)

7 vågrätt: NOLLDAGSATTACK Utnyttjande av en sårbarhet innan tillverkaren har släppt en korrigering (14 bokstäver)

LODRÄTT

1 lodrätt: RAMVERK Strukturerade riktlinjer, som NIST, som används för att hantera cyberrisker (7 bokstäver)

2 lodrätt: HONUNGSFAT Lockbetessystem som sätts upp för att locka och analysera illasinnade aktörer (10 bokstäver)

3 lodrätt: INCIDENTPLAN Strukturerad plan för att hantera och begränsa säkerhetsintrång (12 bokstäver)

4 lodrätt: BRANDVÄGG Nätverksbarriär som filtrerar trafik utifrån säkerhetsregler (9 bokstäver)

5 lodrätt: FLERFAKTOR Säkerhetsvalidering som kräver två eller fler autentiseringsfaktorer (10 bokstäver)

6 lodrätt: RANSOMWARE Skadlig kod som krypterar data och kräver betalning för dekryptering (10 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1. RWMOARAESN — RANSOMWARE
2. DOALGCNASKTTAL — NOLLDAGSATTACK
3. BVDRÄGNGA — BRANDVÄGG
4. NIGEHY — HYGIEN
5. TARLRKFFOE — FLERFAKTOR
6. ANUSFHOGTN — HONUNGSFAT
7. TPDINNNLACEI — INCIDENTPLAN
8. AVKRREM — RAMVERK

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"SKYDDA SYSTEMET MED FLERA FAKTORER"

Facit till fallstudierna

A Fallstudie 1: Återhämtningsstrategi efter ransomware

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: Ett företagsnätverk är infekterat med ransomware som låser kritiska databaser. Angriparna kräver 100 000 USD i kryptovaluta. Företaget har offline-backuper från 24 timmar tillbaka.
- Rekommenderad strategi och lösning: Risker med att betala: Att betala garanterar inte att filerna dekrypteras, märker företaget som ett mål som betalar och finansierar brottslig verksamhet. Återhämtningsstrategi: Teamet bör isolera infekterade värdar, rensa kompromitterade servrar och återställa data från offline-backuper. De måste täppa till den ursprungliga intrångsvägen (nätfiske eller sårbarhet) för att förhindra omedelbar ny infektion.

B Fallstudie 2: Försvar mot credential stuffing

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En onlinetjänst utsätts för en attack med inloggningsuppgifter (credential stuffing), där hackare testar miljontals kombinationer av användarnamn och lösenord som stulits från andra webbplatser.
- Rekommenderad strategi och lösning: Mekanism: Angripare utnyttjar att lösenord återanvänds på olika webbplatser och använder automatiserade botar för att logga in på användarkonton. Försvar: 1. Multifaktorautentisering (MFA) blockerar inloggningsförsök även om lösenordet är korrekt. 2. Hastighetsbegränsning och CAPTCHA hindrar automatiserad bottrafik från att översvämma inloggningsslutpunkter.