Namn: _____ Datum: _____ Poäng: _____

Lösenordsläckor och säkerhet för inloggningsuppgifter

Credential stuffing, dataintrång, hashalgoritmer, multifaktorautentisering och lösenordssäkerhet.

LÄRANDEÖVERSIKT: LÖSENORDSLÄCKOR

SÄKRAD
DATAKRYPTERING
256-bitars AES-standard

EFTERLEVANDE
GLOBALA STANDARDER
Ramverken GDPR och CCPA

ZERO TRUST
ÅTKOMSTPOLICY
Multifaktorautentisering

Välkommen! Det här aktivitetshäftet guidar dig genom lösenordsläckor och säkerhet för inloggningsuppgifter. Du utforskar credential stuffing, dataintrång, hashalgoritmer, flerfaktorsautentisering och lösenordshanterare.

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/losenord-lacker/

Din inlärningsplan för lösenordssäkerhet

- Förstå riskerna med exponerade inloggningsuppgifter på forum på darkwebben.
- Inför multifaktorautentisering (MFA) och övervakning av kompromitterade inloggningsuppgifter.
- Utforma säkerhetsförsvar för företag mot riktade bedrägerier med social manipulation.

INSTRUKTIONER FÖR GUIDEN OM LÖSENORDSLÄCKOR

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

LÖSENORDSLÄCKOR OCH SKYDD AV INLOGGNINGSUPPGIFTER (INTRODUKTION)

Lösenordsläckor avslöjar användares inloggningsuppgifter på offentliga webbplatser och på darkweb. Unika lösenord från en lösenordshanterare, kontroll mot läckta lösenord och flerfaktorsautentisering (MFA) minskar risken för credential stuffing, medan saltad, långsam hashning av lösenord begränsar skadan om en lösenordsdatabas stjäls.

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

Kontrollpunkt 1: Utmaning med flerval

1. Vad är credential stuffing?

- A. Att använda automatisering för att testa läckta kombinationer av användarnamn och lösenord på flera webbplatser
- B. Att kryptera lokala lagringsfiler för databaser
- C. Att överbelasta webbservrar med nätverkstrafikförfrågningar
- D. Att i hemlighet övervaka tangentbordsinmatning

2. Vilken algoritm listar OWASP som sitt förstahandsval för att lagra lösenord i dag?

- A. Argon2id
- B. MD5
- C. SHA-1
- D. ROT13

3. Hur minskar multifaktorautentisering (MFA) risken med lösenordsläckor?

- A. Den kräver en ytterligare verifieringsfaktor, så ett stulet lösenord räcker inte
- B. Den byter automatiskt lösenordet varje timme
- C. Den krypterar användarnamnet under överföringen
- D. Den varnar kreditupplysningsföretaget om bedrägliga förfrågningar

4. Vad är en datadump efter dataintrång?

- A. En samling läckta användaruppgifter som publiceras på nätet eller säljs på hackerforum
- B. En säkerhetskopia av databasfiler lagrad externt
- C. En tillfällig cache med webbserverloggar
- D. Ett administrativt verktyg för att återställa användares lösenord

5. Vilken roll har en lösenordshanterare?

- A. Att skapa och lagra unika, starka lösenord för varje konto
- B. Att övervaka nätverkstrafik efter lösenordsläckor
- C. Att blockera automatiserade brute force-attacker i gatewayen
- D. Att skanna databasens lagringsblock efter okrypterade lösenord

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Att återanvända lösenord på flera konton ökar risken för credential stuffing.

- ○ Sant
- ○ Falskt

7 Fråga 7

7. SHA-1 är en rekommenderad hashfunktion för modern lagring av lösenord.

- ○ Sant
- ○ Falskt

8 Fråga 8

8. Att enbart kräva komplexa lösenord (utan MFA) stoppar credential stuffing helt.

- ○ Sant
- ○ Falskt

9 Fråga 9

9. Verktyg för övervakning av darknet söker igenom internet efter komprometterade företagsuppgifter.

- ○ Sant
- ○ Falskt

10 Fråga 10

10. Saltade hashvärden lägger till unika slumpdata till lösenord före hashning för att motverka angrepp med regnbågstabeller.

- ○ Sant
- ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

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

1. Att testa läckta inloggningsuppgifter mot många webbapplikationer kallas credential _____ .

2. En långsam, adaptiv hashalgoritm för lösenord som OWASP fortfarande godkänner är _____ .

3. Att konfidentiella databasfiler exponeras på internet är ett _____ .

4. Att lägga till slumpmässiga värden till lösenord före hashning kallas _____ .

5. En säker lokal databas för användaruppgifter är en _____ för lösenord.

6. Att lägga till ett andra verifieringssteg vid inloggning ingår i autentisering med flera faktorer, förkortat _____ .

ORDBANK

BCRYPT | DATAINTRÅNG | HANTERARE | MFA | NÄTFISKE | RAINBOW-TABELL | SALTNING | STUFFING

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av säkerhetsbegrepp

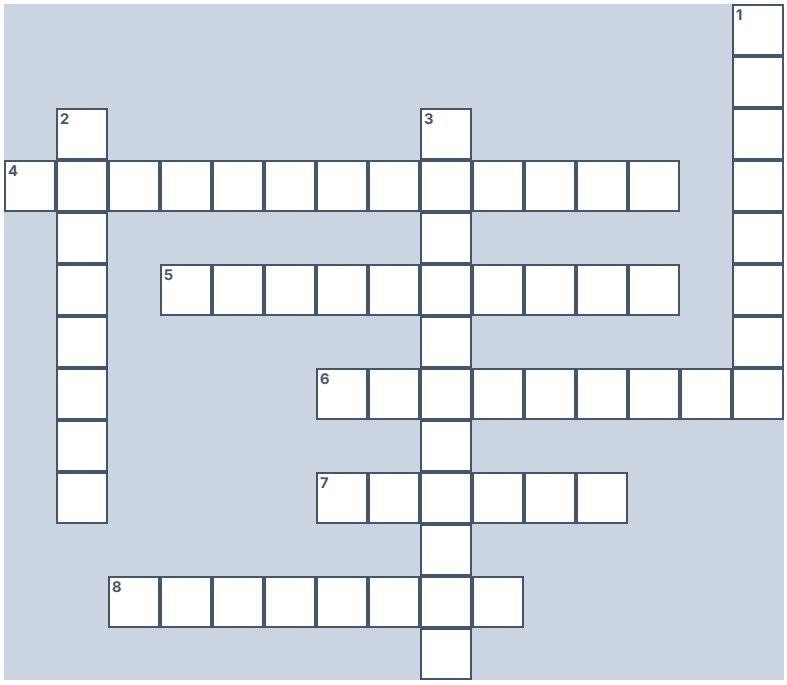
MATCHNING AV DEFINITIONER

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

☐	1. STUFFING	A	Förberäknad tabell över lösenordshashar.
☐	2. BCRYPT	B	Inloggningskontroll med flera faktorer.
☐	3. INTRÅNG	C	Verktyg för lagring av inloggningsuppgifter.
☐	4. SALTNING	D	Obehörig exponering av databaser.
☐	5. HANTERARE	E	Social manipulation för att stjäla inloggningar.
☐	6. MFA	F	Testning av läckta inloggningsuppgifter.
☐	7. REGNBÅGE	G	Att lägga till slumpmässigt salt i lösenordshashen.
☐	8. NÄTFISKE	H	Långsam algoritm för lösenordshashning.

Kontrollpunkt 5: Korsord

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



VÅGRÄTT

4. Förberäknad tabell över lösenordshashar. (13)

5. Inloggningskontroll med flera faktorer. (10)

6. Verktyg för lagring av inloggningsuppgifter. (9)

7. Långsam hashalgoritm för lösenord. (6)

8. Testning av läckta inloggningsuppgifter. (8)

LODRÄTT

1. Social manipulation för att stjäla inloggningar. (8)

2. Tillägg av slumpmässigt salt till lösenordets hash. (8)

3. Obehörig exponering av en databas. (11)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

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

VÅGRÄTT

4 vågrätt: Förberäknad tabell över lösenordshashar. (13 bokstäver):

5 vågrätt: Inloggningskontroll med flera faktorer. (10 bokstäver):

6 vågrätt: Verktyg för lagring av inloggningsuppgifter. (9 bokstäver):

7 vågrätt: Långsam hashalgoritm för lösenord. (6 bokstäver):

8 vågrätt: Testning av läckta inloggningsuppgifter. (8 bokstäver):

LODRÄTT

1 lodrätt: Social manipulation för att stjäla inloggningar. (8 bokstäver):

2 lodrätt: Tillägg av slumpmässigt salt till lösenordets hash. (8 bokstäver):

3 lodrätt: Obehörig exponering av en databas. (11 bokstäver):

Kontrollpunkt 6: Dolt ordsök

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

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

ORDLISTA

STUFFING BCRYPT DATAINTRÅNG SALTNING HANTERARE FLERFAKTOR RAINBOWTABELL NÄTFISKE

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. STUFFING**
- **B. BCRYPT**
- **C. DATAINTRÅNG**
- **D. SALTNING**
- **E. HANTERARE**
- **F. FLERFAKTOR**
- **G. RAINBOWTABELL**
- **H. NÄTFISKE**

DEFINITIONER OCH MATCHNINGSFÄLT

_____ 1. Social manipulation för att stjäla inloggningar.

_____ 2. Obehörig exponering av en databas.

_____ 3. Långsam hashalgoritm för lösenord.

_____ 4. Förberäknad tabell över lösenordshashar.

_____ 5. Testning av läckta inloggningsuppgifter.

_____ 6. Tillägg av slumpmässigt salt till lösenordets hash.

_____ 7. Verktyg för lagring av inloggningsuppgifter.

_____ 8. Inloggningskontroll med flera faktorer.

Kontrollpunkt 7: Utmaning med blandade ord

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

1. NFFSITGU
2. IGADNNTÅRTA
3. HREAAETRN
4. OLAITBLWEBRAN
5. YRTBPC
6. NGTISNAL
7. LRFKATORFE
8. FÄIENKST

Bonusaktivitet: Tänk snabbt

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

1	Säkra vanor du kan börja med i dag			
2	Regler för ett starkt lösenord			
3	Lösenordshanterare du känner till			
4	Säkerhetsverktyg du känner till			
5	Varningstecken i ett e-postmeddelande			
6	Roliga ord till en lång lösenfras			
7	Sätt att logga in utan lösenord			
8	Information du aldrig bör dela			
9	Skäl till att uppdatera programvara			
10	Saker att göra när ett lösenord läcker			
11	Konton som behöver MFA			
12	Platser där lösenord aldrig bör sparas			
13	Tecken på att en dator är infekterad			
14	Dåliga lösenord som folk använder			
15	Saker du säkerhetskopierar			

Kontrollpunkt 8: Fallstudier om cybersäkerhet

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

FALLSTUDIE 1: ÅTGÄRDER VID LÄCKA AV FÖRETAGSUPPGIFTER

👷

Scenario: En tjänst för övervakning av darkweb varnar en organisation för att en databasdump med lösenord för företagets systemadministratörer har publicerats online.

Diskussionsfråga: Analysera riskerna med läckan av inloggningsuppgifter och föreslå en strategi för administrativ återställning.

FALLSTUDIE 2: INFÖRA STANDARDER FÖR LÖSENORDSHASHNING

👷

Scenario: En företagsdatabas lagrar för närvarande användarnas lösenord med föråldrade MD5-hashar utan kryptografiskt salt, vilket gör dem sårbara för snabb utvinning.

Diskussionsfråga: Utforma en migreringsstrategi för att uppgradera databasens hashalgoritm.

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	12	28	3	11	20	1

12	29	19	5	14	15	18	4	13	5	4

6	12	5	18	6	1	11	20	15	18	19	11	15	14	20	18	15	12	12

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 en lösenordsläcka?

En lösenordsläcka uppstår när användares inloggningsuppgifter exponeras genom dataintrång eller felkonfigurerade servrar.

Q2: Hur hittar hackare läckta lösenord?

Hackare söker igenom forum på darkweb, offentliga databasdumpar och paste-webbplatser där data från intrång publiceras [8].

Q3: Är det farligt att återanvända lösenord?

Ja, eftersom hackare kan testa samma inloggningsuppgifter på tusentals andra plattformar om en webbplats kompromitteras [3].

Q4: Vad är ett kryptografiskt salt?

Ett salt är slumpmässiga data som läggs till i ett lösenord före hashning, vilket gör attacker med förberäknade tabeller ineffektiva [2].

Q5: Varför är MD5 föråldrat?

MD5 är en snabb, föråldrad allmän hashfunktion, så angripare kan testa lösenordsgissningar extremt snabbt, särskilt när hasharna är osaltade [2].

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

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

Q6: Hur skyddar en lösenordshanterare användare?

Den genererar automatiskt komplexa, unika inloggningsuppgifter för varje webbplats, vilket minskar mänskliga minnesfel och återanvändning.

Q7: Vad är en brute force-attack?

En attack som systematiskt testar varje möjlig teckenkombination tills rätt lösenord hittas [4].

Q8: Hur hjälper kontolåsning?

Spärr eller hastighetsbegränsning bromsar upprepade gissningar online och minskar tillsammans med övervakning och MFA risken för brute force-attacker [4].

Q9: Är huvudlösenord säkra?

De är säkra om de är lösenfraser med hög entropi som aldrig återanvänds i andra webbsystem.

Q10: Bör lösenord bytas regelbundet?

NIST säger att man inte ska tvinga fram periodiska byten; byt vid belägg för komprometterande och prioritera längd, blocklistor och MFA [1].

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

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

Q1: Hur jämförs Argon2 med bcrypt?

OWASP listar Argon2id som förstahandsval; dess minneskrävande inställningar motstår knäckning med GPU och ASIC bättre än bcrypt [2].

Q2: Vad är nyckelstärkning (key stretching)?

En teknik som upprepar en hashningsalgoritm tusentals gånger för att fördröja lösenordsverifieringen och göra knäckning kostsam [2].

Q3: Hur fungerar regnbågstabeller?

De är förberäknade uppslagstabeller som kopplar klartextlösenord till deras hashvärden och används för att snabbt vända osaltade hashar [2].

Q4: Vad är återvinning av inloggningsuppgifter?

Att återanvända stulna kombinationer av användarnamn och lösenord från ett intrång för att försöka komma åt andra tjänster, särskilt där människor har återanvänt lösenord [3].

Q5: Kan lösenordshanterare hackas?

Ja. Många använder kryptering med noll kunskap (zero-knowledge), så ett intrång på servern avslöjar bara krypterade valv, men svaga huvudlösenord kan ändå knäckas offline.

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 ordboksattack?

En brute force-variant som testar vanliga ord, fraser och tidigare läckta lösenord i stället för slumpmässiga bokstäver.

Q7: Varför föredras lösenfraser?

Lösenfraser använder flera slumpmässiga ord, vilket ger hög entropi som är lätt för människor att komma ihåg men beräkningsmässigt dyr att knäcka [1].

Q8: Hur påverkar enkel inloggning (SSO) läckta lösenord?

SSO minskar lösenordsvildväxten, men identitetsleverantören blir ett mycket värdefullt mål som kräver stark, helst nätfiskeresistent MFA [6].

Q9: Vad är sessionskapning?

En angripare skaffar eller missbrukar en giltig sessionstoken för att utge sig för att vara en inloggad användare utan att behöva lösenordet igen [5].

Q10: Hur upptäcker du password spraying?

Genom att leta efter samma få lösenord som prövas mot många konton, ofta långsamt för att hålla sig under spärrgränserna [7].

Del 11: 10 verkliga fakta och insikter om cybersäkerhet

Gå igenom verkliga fakta om säkerhetsintrång, försvarsmekanismer och efterlevnadsstandarder.

1. SÄKERHETSINSIKT

NIST SP 800-63B kräver att nya lösenord kontrolleras mot blocklistor över vanliga och komprometterade lösenord [1].

2. SÄKERHETSINSIKT

Dumpen "Collection #1" från 2019 slog ihop data från många tidigare intrång till en enda enorm fil med par av e-postadresser och lösenord [8].

3. SÄKERHETSINSIKT

NIST kräver numera att lösenord som används som enda autentiseringsfaktor är minst 15 tecken långa [1].

4. SÄKERHETSINSIKT

ASIC-hårdvara kan beräkna miljarder SHA-256-hashar per sekund, vilket gör rå SHA-hashning osäker för användarlösenord [2].

5. SÄKERHETSINSIKT

Unika salter innebär att två användare med exakt samma lösenord får olika hashvärden i databasen [2].

6. SÄKERHETSINSIKT

Många lösenordshanterare krypterar valvets data lokalt med stark kryptografi som härleds från användarens huvudlösenord.

7. SÄKERHETSINSIKT

Credential stuffing fungerar eftersom många återanvänder samma lösenord på konton för e-handel, bank och e-post [3].

8. SÄKERHETSINSIKT

NIST SP 800-63B säger att verifierare inte ska kräva periodiska lösenordsbyten, bara byten efter belägg för att lösenordet har komprometterats [1].

9. SÄKERHETSINSIKT

Att lägga till en enda versal och ett symbol i ett kort lösenord stoppar inte moderna automatiserade GPU-ordlisteattacker [1].

10. SÄKERHETSINSIKT

MFA kan blockera många credential stuffing-försök även efter att ett lösenord har läckt; nätfiskeresistent MFA är starkare än SMS-koder [3].

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. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[2] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

[3] OWASP. (n.d.). Credential Stuffing Prevention Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

[4] OWASP. (n.d.). Authentication Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[5] OWASP. (n.d.). Session Management Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[6] CISA. (2022). Implementing Phishing-Resistant MFA (fact sheet).

https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[7] CISA. (2018). Brute Force Attacks Conducted by Cyber Actors (Alert TA18-086A).

https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors

[8] Hunt, T. (2019). The 773 Million Record "Collection #1" Data Breach. Troy Hunt.

https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Facit: Kontrollpunkt 1 – Flerval

1 Fråga 1

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Credential stuffing använder automatisering för att prova läckta kombinationer av användarnamn och lösenord på andra webbplatser [3].

2 Fråga 2

Rätt svar: A

ANTECKNING FÖR LÄRAREN

OWASP rekommenderar Argon2id först; bcrypt är främst till för äldre system där Argon2id eller scrypt inte finns tillgängliga [2].

3 Fråga 3

Rätt svar: A

ANTECKNING FÖR LÄRAREN

MFA kräver en ytterligare faktor, så ett stulet lösenord ensamt kan inte låsa upp kontot [3].

4 Fråga 4

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Dataintrångsdumpar är läckta samlingar av inloggningsuppgifter, till exempel sammanställningen Collection #1 från 2019 [8].

5 Fråga 5

Rätt svar: A

ANTECKNING FÖR LÄRAREN

En lösenordshanterare genererar och lagrar ett unikt, starkt lösenord för varje konto och förhindrar återanvändning [3].

Facit: Kontrollpunkt 2 – Sant eller falskt

6 Fråga 6

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Sant: återanvända lösenord låter angripare spela upp inloggningsuppgifter som läckt från en webbplats på andra webbplatser [3].

7 Fråga 7

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: SHA-1 är en snabb hash; OWASP rekommenderar i stället Argon2id, scrypt, bcrypt eller PBKDF2 [2].

8 Fråga 8

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: komplexitetsregler ensamma kan inte stoppa stuffing med återanvända läckta lösenord; MFA behövs [3].

9 Fråga 9

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Sant: övervakningstjänster söker igenom dataintrångsdumpar och källor på darkweb efter exponerade inloggningsuppgifter [8].

10 Fråga 10

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Sant: ett unikt salt per lösenord gör förberäknade regnbågstabeller ineffektiva [2].

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

F 1. STUFFING	H 2. BCRYPT	D 3. INTRÅNG	G 4. SALTNING
C 5. HANTERARE	B 6. MFA	A 7. REGNBÅGE	E 8. NÄTFISKE

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 STUFFING	2 BCRYPT	3 DATAINTRÅNG	4 SALTNING
5 HANTERARE	6 MFA		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 H – NÄTFISKE	2 C – DATAINTRÅNG	3 B – BCRYPT	4 G – RAINBOWTABELL
5 A – STUFFING	6 D – SALTNING	7 E – HANTERARE	8 F – FLERFAKTOR

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara STUFFING, BCRYPT och INTRÅNG med egna ord och ge ett exempel på varje.

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

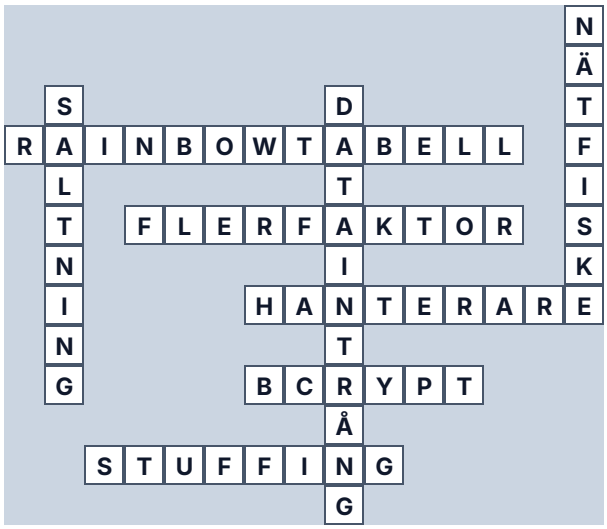
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

4 vågrätt: RAINBOWTABELL Förberäknad tabell över lösenordshashar. (13 bokstäver)

5 vågrätt: FLERFAKTOR Inloggningskontroll med flera faktorer. (10 bokstäver)

6 vågrätt: HANTERARE Verktyg för lagring av inloggningsuppgifter. (9 bokstäver)

7 vågrätt: BCRYPT Långsam hashalgoritm för lösenord. (6 bokstäver)

8 vågrätt: STUFFING Testning av läckta inloggningsuppgifter. (8 bokstäver)

LODRÄTT

1 lodrätt: NÄTFISKE Social manipulation för att stjäla inloggningar. (8 bokstäver)

2 lodrätt: SALTNING Tillägg av slumpmässigt salt till lösenordets hash. (8 bokstäver)

3 lodrätt: DATAINTRÅNG Obehörig exponering av en databas. (11 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1. NFFSITGU — **STUFFING**
2. IGADNNTÅRTA — **DATAINTRÅNG**
3. HREAAETRN — **HANTERARE**
4. OLAITBLWEBRAN — **RAINBOWTABELL**
5. YRTBPC — **BCRYPT**
6. NGTISNAL — **SALTNING**
7. LRFKATORFE — **FLERFAKTOR**
8. FÄIENKST — **NÄTFISKE**

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"SKYDDA LÄCKTA LÖSENORD MED FLERFAKTORSKONTROLL"

Facit till fallstudierna

A Fallstudie 1: Åtgärder vid läcka av företagsuppgifter

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En tjänst för övervakning av den mörka webben varnar en organisation för att en datadump med lösenord för företagets systemadministratörer har publicerats på nätet.
- Rekommenderad strategi och lösning: Återkalla alla aktiva administratörssessioner och återställ inloggningsuppgifterna med en generator med hög entropi. Kräv nätfiskeresistent MFA på administratörsportaler [6], rotera påverkade API-nycklar, granska inloggningsloggar, hitta den ursprungliga exponeringen och kontrollera andra privilegierade konton.

B Fallstudie 2: Införa standarder för lösenordshashning

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En företagsdatabas lagrar för närvarande användarlösenord med föråldrade MD5-hashar utan kryptografiskt salt, vilket gör dem sårbara för snabb utvinning.
- Rekommenderad strategi och lösning: Använd Argon2id (eller bcrypt i äldre system) med ett unikt salt per användare [2]. Linda in de befintliga MD5-hasharna i den nya algoritmen nu, hasha om direkt vid varje användares nästa inloggning och tvinga fram återställning för konton som varit inaktiva länge.