שם: _____ תאריך: _____ ציון: _____

הגנה על נתונים ואחסון ארגוני מדריך אבטחה

מיסוך נתונים, טוקניזציה, הצפנה במנוחה לעומת הצפנה בהעברה, גיבויים לא מקוונים

סקירת למידה: הגנת נתונים

ברוכים הבאים! חוברת הפעילויות הזו תדריך אתכם דרך תקנים ובקרות להגנה על נתונים. תחקרו הצפנת דיסק מלאה, בקרות גישה מאובטחות, גיבויי חומרה, מצב אבטחת ענן וטכניקות הסתרת נתונים (data masking).

אובטח

הצפנת נתונים

תקן AES של 256 סיביות

תואם

תקנים עולמיים

מסגרות GDPR ו-CCPA

אפס אמון

מדיניות גישה

אימות רב-גורמי

נקודות הביקורת בדף העבודה

- [ ] **חלק 1-4: שלטו באבטחת סייבר ובמניעת איומים.**
- [ ] **חלק 5-7: פתרו תשבצים ופאזלי חיפוש מילים.**
- [ ] **חלק 8-9: פתרו מקרי בוחן ואתגר צופן.**
- [ ] **חלק 10: סקרו את דפי השאלות הנפוצות הבסיסיים והמתקדמים.**
- [ ] **חלק 11: חקרו 10 עובדות מעניינות מהעולם האמיתי.**
- [ ] **בונוס: אתגר חשבו מהר**

פתחו את מדריך אבטחת הסייבר של VPN.com

URL: https://www.vpn.com/cybersecurity/data-protection/

מפת הלמידה שלכם: אסטרטגיית הגנה על נתונים

- הבחינו בין טכניקות של מיסוך נתונים וטוקניזציה.
- יישמו הצפנה במנוחה לכונני אחסון והצפנה במעבר באמצעות TLS.
- תכננו מערכות גיבוי לא מקוונות ומבודדות מהרשת להגנה מפני כופרה.

הוראות למדריך הגנת נתונים

ענו על שאלות אמריקאיות ועל שאלות נכון/לא נכון, השלימו את המשפטים החסרים בעזרת בנק המילים, התאימו הגדרות ופתרו את התשבץ ואת תפזורת המילים. יישמו את הידע שלכם בנושא הגנה על נתונים. ולסיום, פעילות הבונוס "חשבו מהר".

הגנת נתונים ואבטחת אחסון ארגוני (מבוא)

הגנה על נתונים שומרת על נכסי הנתונים של הארגון באמצעות מיסוך, טוקניזציה, הצפנת מסדי נתונים במנוחה ופרוטוקולי העברה מאובטחים. תכנון גיבויים מבודדים מהרשת עוזר להבטיח שניתן יהיה לשחזר מסדי נתונים מרכזיים במקרה של חדירה פעילה.

קראו כל נקודת ביקורת בעיון ובחרו או כתבו את התגובה הנכונה.

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. מהי המטרה העיקרית של מיסוך נתונים?

- A. החלפת מזהים רגישים בתווים בדיוניים אך ריאליסטיים כדי להגן על הפרטיות
- B. דחיסת קובצי מסד נתונים גדולים כדי לחסוך מקום אחסון פיזי בשרת
- C. מחיקת הודעות דוא"ל ישנות של אנשי קשר של לקוחות ממערכות גיבוי ארכיוניות
- D. הסתרת כתובת ה-IP הציבורית של שרת מסד הנתונים מסריקות אינטרנט

2. איזה מנגנון מצפין קבצים המאוחסנים בכונן הקשיח של שרת מסד נתונים?

- A. הצפנת דיסק מלאה במנוחה
- B. פרוטוקולי לחיצת יד של סשן TLS בזמן המעבר
- C. כללי העברת שרתי שמות של Dynamic DNS
- D. אימות רב-שלבי באמצעות מפתחות חומרה

3. מה מייצג נתונים בתנועה?

- A. מנות נתונים שנעות בין נתבים ומתגים ברשת
- B. יומני עסקאות של מסד נתונים המאוחסנים בכונן גיבוי קר
- C. קובצי משתמש בארכיון שנשמרו בכספת ענן מבודדת
- D. קובצי תצורת מערכת סטטיים באחסון של מחשב שולחני מקומי

4. מדוע גיבוי לא מקוון סדיר קריטי להגנה מפני כופרה?

- A. הוא מספק עותק נקי ולא מקוון לשחזור קבצים בלי לשלם כופר
- B. הוא מונע מהאקרים לסרוק תצורות של פורטים פתוחים
- C. הוא מגדיל את מהירויות רוחב הפס של שידור הרשת המקומית
- D. הוא מבצע אוטומציה של יומני הסכמה לעוגיות בדפדפנים

5. מה עושה טוקניזציה של נתונים?

- A. הוא מחליף מספרי כרטיס רגישים באסימונים אקראיים לא רגישים
- B. הוא מנתב תעבורת אינטרנט דרך מספר צמתי onion מאובטחים
- C. הוא סורק ספריות מערכת בחיפוש נוזקות מבוססות חתימה
- D. הוא מבקר את זמני ההתחברות של מנהלי מסד הנתונים

נקודת ביקורת 2: אתגר נכון או לא נכון

6 שאלה 6

6. מיסוך נתונים משנה רשומות במסד הנתונים באופן קבוע בסביבות ייצור.

נכון ○ לא נכון ○

7 שאלה 7

7. גיבויים מחוץ לאתר חייבים להיות מבודדים מרשת החברה הראשית כדי למנוע התפשטות של כופרה.

נכון ○ לא נכון ○

8 שאלה 8

8. אישורי SSL/TLS מאבטחים מסדי נתונים על ידי הצפנת נתונים שמאוחסנים במנוחה על מדיה פיזית.

נכון ○ לא נכון ○

9 שאלה 9

9. גישת רשת Zero Trust (ZTNA) מאמתת את זהותו של כל משתמש לפני מתן גישה למסד הנתונים.

נכון ○ לא נכון ○

10 שאלה 10

10. טוקניזציה מבוססת כספת שומרת את ערכי הכרטיס המקוריים בכספת אסימונים מרכזית ומאובטחת.

נכון ○ לא נכון ○

נקודת ביקורת 3: השלמת מונחי מפתח

קראו כל משפט שלהלן והשלימו את החסר במונח הנכון מבנק המילים.

1. החלפת שמות אישיים במציינים מציאותיים נקראת _____ נתונים.
2. הצפנת בלוקי אחסון פיזיים מגינה על נכסי מסד נתונים _____ .
3. פרוטוקולי TLS מצפינים חבילות נתונים פעילות הנעות _____ .
4. הרשאות מבוססות תפקיד מגבילות אילו משתמשים יכולים לקבל _____ למסד הנתונים.
5. שחזור קבצי חברה נקיים לאחר פריצה מחייב _____ מאובטח במצב לא מקוון.
6. ביקורת על תצורות ענן בוחנת את _____ של הארגון.

בנק מילים

במעבר | במצב מנוחה | גיבוי | גישה | מיסוך | עמדת האבטחה | פריצה | ציות

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים באבטחה

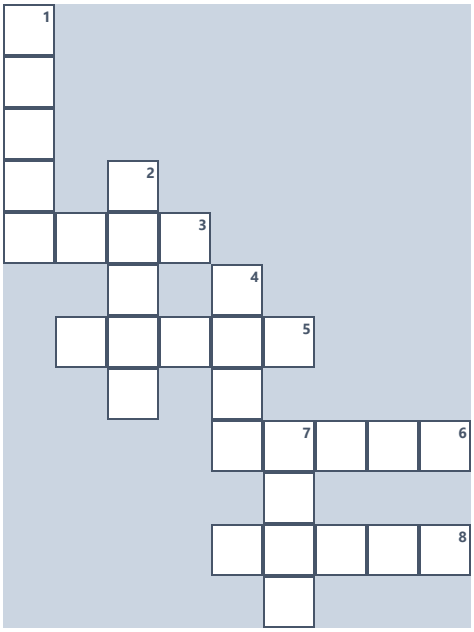
התאמת הגדרות

התאימו כל מונח אוצר מילים בצד ימין להגדרה הנכונה שלו בצד שמאל על ידי כתיבת האות המתאימה (A-H) בתיבת הקלט הניתנת למילוי.

1. הצפנה	A	יצירת עותקים מאובטחים של נתונים מחוץ לאתר לשחזור במקרה של כשלי מערכת.
2. גיבוי	B	הפיכת טקסט גלוי לטקסט מוצפן בלתי קריא כך שנתונים שיורטו יישארו פרטיים.
3. צמצום	C	מצב האבטחה הקולקטיבי ומוכנות ההגנה של הענן של ארגון.
4. גישה	D	עמידה בתקנים רגולטוריים כמו GDPR או CCPA לניהול מידע פרטי של משתמשים.
5. מצב אבטחה	E	אירוע אבטחה שבו ניגשים לנתונים מוגנים או חושפים אותם ללא הרשאה.
6. פריצה	F	הגבלת הרשאות קריאה וכתיבה במסד נתונים לתפקידי משתמש מאומתים.
7. ציות	G	החלפת תווים רגישים בשדות מסד נתונים כדי להגן על זהויות אישיות.
8. הסתרה	H	הגבלת איסוף הנתונים האישיים למינימום ההכרחי לפעילות.

נקודת ביקורת 5: תשבץ

פתרו את התשבץ על ידי הקלדת אותיות בתיבות הלבנות הפעילות. המספרים מתאימים לרמזים שלהלן.



מאונן

3. המצב הכולל של האבטחה ומוכנות ההגנה של הענן של הארגון. (4)

5. יצירת עותקים מאובטחים מחוץ לאתר כדי לשחזר במקרה של כשלי מערכת. (5)

6. אירוע אבטחה שבו נתונים מוגנים נגישים או נחשפים ללא הרשאה (5)

8. החלפת תווים רגישים בשדות מסד הנתונים כדי להגן על זהויות אישיות. (5)

מאונך

1. הפיכת טקסט גלוי לטקסט מוצפן בלתי קריא כך שנתונים שנחטפו נשארים פרטיים (5)

2. הגבלת איסוף הנתונים האישיים למינימום ההכרחי לפעילות. (5)

4. הגבלת הרשאות קריאה וכתיבה במסד הנתונים לתפקידי משתמש מאומתים. (4)

7. עמידה בתקנים רגולטוריים כמו GDPR או CCPA בניהול מידע פרטי של משתמשים. (4)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

משתמשי קורא מסך ומקלדת יכולים להקליד את תשובות התשבץ ישירות בשדות הטקסט שלהלן.

מאוזן

3 מאוזן: המצב הכולל של האבטחה ומוכנות ההגנה של הענן של הארגון. (4 אותיות):

5 מאוזן: יצירת עותקים מאובטחים מחוץ לאתר כדי לשחזר במקרה של כשלי מערכת. (5 אותיות):

6 מאוזן: אירוע אבטחה שבו נתונים מוגנים נגישים או נחשפים ללא הרשאה (5 אותיות):

8 מאוזן: החלפת תווים רגישים בשדות מסד הנתונים כדי להגן על זהויות אישיות. (5 אותיות):

מאונך

1 מאונך: הפיכת טקסט גלוי לטקסט מוצפן בלתי קריא כך שנתונים שנחטפו נשארים פרטיים (5 אותיות):

2 מאונך: הגבלת איסוף הנתונים האישיים למינימום ההכרחי לפעילות. (5 אותיות):

4 מאונך: הגבלת הרשאות קריאה וכתיבה במסד הנתונים לתפקידי משתמש מאומתים. (4 אותיות):

7 מאונך: עמידה בתקנים רגולטוריים כמו GDPR או CCPA בניהול מידע פרטי של משתמשים. (4 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

מצאו את 8 מונחי המפתח בלוח שלהלן. מילים יכולות להופיע אופקית, אנכית או באלכסון.

א	ו	ש	ה	ז	ש	ק	ם	צ	ד	ל	ס	נ	י	ז
ס	ה	כ	ב	ק	ד	א	פ	ג	י	נ	ז	ך	ד	ד
א	צ	מ	ז	ח	צ	מ	ה	נ	י	ה	ס	י	ד	ב
פ	י	ך	א	ז	ט	ר	ט	ח	ך	ש	נ	פ	ש	א
ע	ר	י	ד	י	ה	ת	ל	ך	ס	ת	ה	ו	ס	כ
ג	פ	פ	ח	ו	צ	מ	צ	ע	ל	ס	צ	י	ו	ת
ת	ע	נ	ג	ק	פ	צ	צ	מ	ה	כ	ט	ב	א	ב
ך	ג	נ	ם	כ	נ	י	ם	כ	צ	ת	ק	י	ד	ע
ו	ל	ט	ד	ח	ה	מ	מ	י	ע	ו	ס	ז	ל	ל
ס	ע	פ	צ	ק	ק	ז	ג	צ	ס	נ	ם	ח	פ	ב
י	ג	י	ב	ו	י	ש	ד	צ	ך	ר	ג	ך	ש	ע
מ	ו	י	ז	ך	ד	מ	ד	ע	ת	ס	ג	ק	מ	ב
א	ך	מ	ד	כ	א	ד	נ	ד	ה	ז	ח	ד	ד	פ
ע	ל	ה	ח	פ	ך	צ	ה	ע	ר	ה	א	ה	א	ע
נ	מ	ס	ק	ת	ע	י	פ	ק	פ	ג	מ	ם	ב	ו

רשימת מילים

הצפנה | גיבוי | צמצום | גישה | עמדה | פריצה | ציות | מיסוך

נקודת ביקורת 6 – פעילות חלופית: התאמת אוצר מילים נגישה

התאימו כל אחד מ-8 מונחי המילון מתפזורת המילים להגדרה הנכונה שלו על ידי כתיבת האות (A-H) במקום הריק.

מונחי אוצר מילים
A. הצפנה
B. גיבוי
C. צמצום
D. גישה
E. עמדה
F. פריצה
G. ציות
H. מיסוך

	הגדרות ושדות התאמה
	1. אירוע אבטחה שבו נתונים מוגנים נגישים או נחשפים ללא הרשאה.
	2. החלפת תווים רגישים בשדות מסד הנתונים כדי להגן על זהויות אישיות.
	3. הגבלת הרשאות קריאה וכתיבה במסד הנתונים לתפקידי משתמש מאומתים.
	4. המצב הכולל של האבטחה ומוכנות ההגנה של הענן של הארגון.
	5. עמידה בתקנים רגולטוריים כמו GDPR או CCPA בניהול מידע פרטי של משתמשים.
	6. הגבלת איסוף הנתונים האישיים למינימום ההכרחי לפעילות.
	7. הפיכת טקסט גלוי לטקסט מוצפן בלתי קריא כך שנתונים שנחטפו נשארים פרטיים.
	8. יצירת עותקים מאובטחים מחוץ לאתר כדי לשחזר במקרה של כשלי מערכת.

נקודת ביקורת 7: אתגר מילים מבולבלות

סדרו מחדש את האותיות שלהלן כדי לחשוף מושגים ומונחים מרכזיים באבטחת סייבר. כתבו את תשובותיכם בתיבות הקלט המסופקות.

1. נ פ ה ה צ
2. צ ס ו צ מ
3. ה ע ד מ
4. ת ו צ י
5. ב י ג ו י
6. ש ה ג י
7. צ ה פ י ר
8. ר מ ס ו י

פעילות בונוס: חשבו מהר

כתבו 3 תשובות לכל קטגוריה. מי שמסיים ראשון את הרשימה מנצח.

1	דברים שמגבים		
2	מילים הקשורות לאבטחת סייבר		
3	אנשים שמותר להם לראות נתונים רגישים		
4	דרכים למחוק נתונים בצורה מאובטחת		
5	מקומות שבהם נשמרים נתונים		
6	דברים שצריך להצפין		
7	נתונים שבית חולים חייב להגן עליהם		
8	סוגי גיבוי		
9	מידע שלעולם אסור לשתף		
10	סימני אזהרה באימייל		
11	הרגלים בטוחים שאפשר להתחיל כבר היום		
12	אנשים שאפשר לבקש מהם עזרה ב-IT		
13	מכשירים שאפשר לפרוץ אליהם		
14	דרכים להגן על נתונים		
15	דברים שיכולים להרוס נתונים		

נקודת ביקורת 8: מקרי בוחן באבטחת סייבר

יישמו את המושגים שלמדתם כדי לפתור את התרחישים מהעולם האמיתי שלהלן.

מקרה בוחן 1: שדרוג הצפנת מסד נתונים ארגוני במצב מנוחה

👷

תרחיש: קמעונאי מקוון שומר מסדי נתונים של עסקאות באחסון ענן בלי הצפנת דיסק מלאה. ביקורת תאימות אחרונה סימנה זאת כסיכון אבטחת נתונים חמור לפי CCPA. תכננו ארכיטקטורת התאוששות.

שאלה לדיון: נתחו את סיכוני התאימות ל-CCPA, והציעו אסטרטגיית הצפנה במנוחה (at-rest).

מקרה בוחן 2: בלימת כופרה ושחזור נתונים

👷

תרחיש: התקפת תוכנת כופר פעילה מצפינה כוננים ברשת מקומית ארגונית. המנהל זיהה את ההדבקה מוקדם. תכננו את צעדי הבלימה וההתאוששות.

שאלה לדיון: פרטו את פעולות הבלימה המיידיות, ותכננו תהליך שחזור מאובטח.

נקודת ביקורת 9: פענוח הצופן

איש מקצוע באבטחת סייבר מגן על נכסי רשת מפני גורמי איום מקוונים. השתמשו במפתח האותיות-למספרים שלהלן כדי לפענח את ההודעה, וכתבו את האותיות המתאימות במקומות הריקים.

מפתח הצפנה של אות למספר

א=1 ב=2 ג=3 ד=4 ה=5 ו=6 ז=7 ח=8 ט=9

י=10 כ=11 ל=12 מ=13 נ=14 ס=15 ע=16 פ=17 צ=18

ק=19 ר=20 ש=21 ת=22 ך=23 ם=24 ן=25 ף=26 ץ=27

24	10	10	9	20	17		24	10	14	6	22	14		12	16		6	14	3	5
						22	6	20	19	2		22	20	7	16	2			

ההודעה המפוענחת:

טיפ: כל מספר מייצג אות עברית אחת מהמפתח שלמעלה.

נקודת ביקורת 10: שאלות נפוצות על אבטחת סייבר – בסיסי (חלק A)

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q1: מהי הגנת נתונים?

זהו תהליך אבטחת נתונים אישיים ועסקיים מפני גישה לא מורשית, אובדן או השחתה באמצעות בקרות טכניות.

Q2: מדוע הצפנת דיסק מלאה חשובה?

הוא מאבטח בלוקי נתונים מאוחסנים בכוננים פיזיים ומונע מכל אחד לקרוא נתונים אם גונבים פיזית את הכונן הקשיח.

Q3: מה ההבדל בין הצפנה במנוחה להצפנה בתנועה?

הצפנה במנוחה מאבטחת קבצים שמורים בכוננים, ואילו הצפנה בהעברה מאבטחת חבילות רשת פעילות העוברות דרך נתבים.

Q4: מהו הסתרת נתונים (data masking)?

הוא מחליף פרטים רגישים (כמו מספרי כרטיס אשראי) בנתונים בדיוניים אך ריאליסטיים לצורכי בדיקה בלי לחשוף רשומות אמיתיות.

Q5: מדוע גיבוי לא מקוון חשוב?

הוא שומר עותק נקי של הקבצים שלכם מבודד מהרשת, מה שעוזר להגן על הגיבויים שלכם מפני הצפנה בידי כופרה.

נקודת ביקורת 10: שאלות נפוצות על אבטחת סייבר – בסיסי (חלק B)

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q6: מהי כספת טוקניזציה של נתונים?

מסד נתונים מאובטח ומבודד שממפה אסימונים אקראיים לערכים הרגישים המקוריים שלהם (כמו מספרי כרטיס אשראי ראשיים).

Q7: מה משמעות גישה למסד נתונים לפי Zero Trust?

המשמעות היא אימות זהות כל משתמש ומצב המכשיר בכל התחברות, במקום לתת אמון בכל מי שנמצא בתוך הרשת.

Q8: כיצד TLS מגן על נתונים בתנועה?

TLS מצפין את מטען הסשן של TCP ומונע מגורמים זדוניים ברשתות ציבוריות לצותת למנות במעבר או לשנות אותן.

Q9: מהי ביקורת גישה למסד נתונים?

התיעוד הרציף של שאילתות מסד נתונים וכניסות כדי לזהות דפוסי גישה לא מורשית או חריגות אבטחה.

Q10: מהי ביקורת מצב אבטחת ענן?

תהליך שמנתח הגדרות ענן כדי לזהות פורטים פתוחים, כללי גישה שהוגדרו באופן שגוי ופערי עמידה בדרישות אבטחה.

נקודת ביקורת 10: שאלות נפוצות על אבטחה – מתקדם (חלק C)

חקרו היבטים טכניים מתקדמים של מסגרות אבטחה, ניתוח נוזקות ועמידה בדרישות נתונים.

Q1: כיצד פועלת הצפנת מעטפה?

הוא מצפין נתונים באמצעות מפתח נתונים, ואז מצפין את מפתח הנתונים הזה באמצעות מפתח ראשי, מה שמפשט את אחסון המפתחות ואת החלפתם.

Q2: מהי הצפנה הומומורפית?

שיטת הצפנה מתקדמת שמאפשרת לבצע פעולות ישירות על נתונים מוצפנים בלי לפענח אותם קודם.

Q3: מדוע נעשה שימוש בהצפנה ברמת עמודה במסד נתונים?

הוא מצפין עמודות רגישות מסוימות (כמו מספרי זהות) בנפרד ומגן עליהן גם אם מנהלים קיבלו גישת קריאה כללית לטבלה.

Q4: מהי מניעת דליפת נתונים (DLP)?

תוכנה המנטרת נקודות יציאה ברשת כדי לזהות ולחסום העברות יוצאות לא מורשות של קבצים רגישים.

Q5: כיצד גיבויי כתיבה-חד-פעמית-קריאה-רבה (WORM) מגנים מפני תוכנות כופר?

גיבויי WORM מונעים מחיקה או שינוי של קבצים למשך זמן קבוע, ובכך מונעים מכופרה להצפין גיבויים קיימים.

נקודת ביקורת 10: שאלות נפוצות על אבטחה – מתקדם (חלק D)

חקרו היבטים טכניים מתקדמים של מסגרות אבטחה, ניתוח נוזקות ועמידה בדרישות נתונים.

Q6: מהו הסיכון בשימוש חוזר במפתחות?

שימוש באותו מפתח הצפנה במסדי נתונים שונים פירושו שפגיעה במפתח אחד חושפת את כל מסדי הנתונים.

Q7: כיצד טוקניזציה של מסד נתונים משפרת את הציות ל-CCPA?

אסימונים מייצרים פסאודונימיזציה של רשומות במערכות שאינן ייצור ומגבילים את החשיפה בפריצה, אך נתונים שעברו אסימון עדיין עשויים להיות מידע אישי.

Q8: מדוע סיווג נתונים קריטי?

הוא מסווג קבצים לפי רמת רגישות ועוזר לארגונים להחיל את ההצפנה ובקרות הגישה החזקות ביותר על נתונים בסיכון גבוה.

Q9: מה תפקידה של החלפת מפתחות?

עדכון סדיר של מפתחות הצפנה מגביל את כמות הנתונים ההיסטוריים החשופים אם מפתח בודד ייפרץ בסופו של דבר.

Q10: כיצד מובלעות מאובטחות (secure enclaves) מגינות על שאילתות מסדי נתונים בזיכרון?

מובלעות מאובטחות (secure enclaves) מבודדות פעולות שאילתה בבלוקי זיכרון המוגנים על ידי המעבד, ומונעות ממנהלי המארח לראות טקסט גלוי ב-RAM.

חלק 11: 10 עובדות ותובנות מהעולם האמיתי על אבטחת סייבר

עיינו בעובדות מהעולם האמיתי על פריצות אבטחה, מנגנוני הגנה ותקני ציות.

1. תובנות על אבטחה

תקנות GDPR נכנסו לתוקף במאי 2018 ושינו את האופן שבו אתרים ברחבי העולם מנהלים הסכמות לעוגיות ומאגרי נתונים אישיים.

2. תובנות על אבטחה

קנס על הפרת GDPR יכול להגיע ל-20 מיליון אירו או ל-4% מהמחזור העולמי, ומהווה חשיפה משפטית משמעותית. [4]

3. תובנות על אבטחה

ה-CCPA נכנס לתוקף בינואר 2020 והקים זכויות צרכן חלוציות בתחום הפרטיות הדיגיטלית בארצות הברית.

4. תובנות על אבטחה

מזעור נתונים מקטין את נפח האחסון במסד הנתונים, מצמצם את עלויות הפעלת השרתים ומפחית את היקף ההשפעה של דליפה.

5. תובנות על אבטחה

מחיקה קריפטוגרפית פותרת את אתגר מחיקת הגיבויים על ידי ניקוי מפתחות במקום עריכת קובצי גיבוי היסטוריים.

6. תובנות על אבטחה

רוב מדינות העולם חוקקו כיום חוקי הגנה על נתונים אישיים כדי להגן על זכויות הפרטיות של הצרכנים.

7. תובנה על אבטחה

טפסי הסכמה עם תיבות מסומנות מראש אסורים במפורש לפי ההגדרות הרגולטוריות האירופיות בתחום פרטיות המידע.

8. תובנה על אבטחה

GDPR מחייב לדווח על הפרות של נתונים אישיים לרשות הפיקוח תוך 72 שעות מרגע ההיוודעות, ככל שניתן. [3]

9. תובנה על אבטחה

גיבוב סיסמאות באמצעות אלגוריתמים איטיים כמו bcrypt או Argon2 מקשה הרבה יותר על פיצוח לא מקוון של גיבובים שנגנבו. [6]

10. תובנות על אבטחה

נתונים במנוחה הם קבצי מסד נתונים שמורים, ואילו נתונים בהעברה הם חבילות שנעות באופן פעיל דרך נתבי רשת.

מקורות והפניות טכניים

מדריך הלימוד והפאזלים האינטראקטיביים נערכו על סמך תקנים גלובליים של NIST, OWASP ותאימות לפרטיות נתונים.

מקורות אקדמיים ותעשייתיים

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

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

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 שאלה 1 — תשובה נכונה: A

הערה למורה

מהי המטרה העיקרית של מיסוך נתונים? → החלפת מזהים רגישים בתווים בדיוניים אך ריאליסטיים כדי להגן על הפרטיות

2 שאלה 2 — תשובה נכונה: A

הערה למורה

איזה מנגנון מצפין קבצים המאוחסנים בכונן הקשיח של שרת מסד נתונים? → הצפנת דיסק מלאה במנוחה

3 שאלה 3 — תשובה נכונה: A

הערה למורה

מה מייצג נתונים בתנועה? → מנות נתונים שנעות בין נתבים ומתגים ברשת

4 שאלה 4 — תשובה נכונה: A

הערה למורה

מדוע גיבוי לא מקוון סדיר קריטי להגנה מפני כופרה? → הוא מספק עותק נקי ולא מקוון לשחזור קבצים בלי לשלם כופר

5 שאלה 5 — תשובה נכונה: A

הערה למורה

מה עושה טוקניזציה של נתונים? → הוא מחליף מספרי כרטיס רגישים באסימונים אקראיים לא רגישים

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 **שאלה 6**

תשובה נכונה: לא נכון

הערה למורה

מיסוך משנה עותקי בדיקה או מסתיר ערכים בזמן השאילתה; רשומות הייצור נשארות ללא שינוי.

7 **שאלה 7**

תשובה נכונה: נכון

הערה למורה

גיבויים מחוץ לאתר חייבים להיות מבודדים מרשת החברה הראשית כדי למנוע התפשטות של כופרה.

8 **שאלה 8**

תשובה נכונה: לא נכון

הערה למורה

תעודות TLS מגינות על נתונים בזמן מעבר; נתונים במנוחה זקוקים להצפנת דיסק, קובץ או מסד נתונים.

9 **שאלה 9**

תשובה נכונה: נכון

הערה למורה

גישת רשת Zero Trust (ZTNA) מאמתת את זהותו של כל משתמש לפני מתן גישה למסד הנתונים.

10 **שאלה 10**

תשובה נכונה: נכון

הערה למורה

טוקניזציה מבוססת כספת שומרת את הערכים המקוריים בכספת אסימונים מאובטחת שממפה כל אסימון בחזרה לנתוניו.

מפתחות אוצר מילים ומחוון הערכה

מחוון הערכה למורה: תנו 1 נקודה לכל התאמה נכונה (סה"כ 8 נקודות) ולכל מונח הקשר (סה"כ 6 נקודות).

נקודת ביקורת 4: מפתח תשובות – התאמת מושגים

B 1. הצפנה	A 2. גיבוי	H 3. צמצום	F 4. גישה
C 5. מצב אבטחה	E 6. פריצה	D 7. ציות	G 8. הסתרה

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 מיסוך	2 במצב מנוחה	3 במעבר	4 גישה
5 גיבוי	6 עמדת האבטחה		

נקודת ביקורת 6 – פעילות חלופית: מפתח תשובות – התאמת אוצר מילים

1 F – פריצה	2 H – מיסוך	3 D – גישה	4 E – עמדה
5 G – ציות	6 C – צמצום	7 A – הצפנה	8 B – גיבוי

הערות לדיון עבור מורים

מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את הצפנה, גיבוי ו-צמצום ונותנים דוגמה לכל אחד מהם.

מקרי בוחן:
בקשו מהתלמידים לבסס את ההמלצות שלהם על עובדות מדף העבודה ולא על דעות.

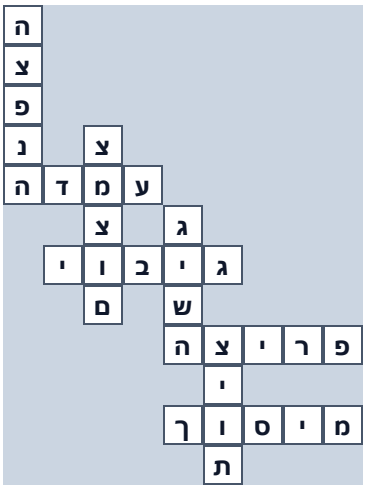
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת

א	ו	ש	ה	ז	ש	ק	ם	צ	ד	ל	ס	נ	י	ז
ס	ה	כ	ב	ק	ד	א	פ	ג	י	נ	ז	ך	ד	ד
א	צ	מ	ז	ח	צ	מ	נ	י	ה	ס	י	ד	ב	
פ	י	ך	א	ז	ך	ט	ח	ך	ש	נ	פ	ש	א	
ע	ר	י	ד	י	ה	ך	ל	ת	ס	ך	ה	ו	ס	כ
ג	פ	פ	ח	ו	צ	מ	ע	ל	ס	צ	י	ו	ת	
ת	ע	נ	ג	ק	פ	צ	מ	צ	ה	כ	ט	ב	א	ב
ך	ג	נ	מ	כ	נ	י	ם	צ	ת	ק	י	ד	ע	
ו	ל	ט	ד	ח	ה	מ	מ	י	ע	ו	ס	ז	ל	ל
ס	ע	פ	צ	ק	ק	ז	ג	צ	ס	נ	ם	ח	פ	ב
י	ג	י	ב	י	ו	י	ד	צ	ך	ר	ג	ך	ש	ע
מ	י	י	ר	ב	ד	ח	ע	ת	ס	ג	ק	ם	ב	
א	ך	מ	ד	כ	א	נ	ד	ה	ז	ח	ד	ך	פ	
ע	ל	ה	ח	פ	ך	צ	ה	ר	ע	ה	א	א	ע	
נ	מ	ס	ק	ת	ע	י	פ	ג	מ	ק	פ	ם	ב	ו

פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

3 מאוזן: עמדה המצב הכולל של האבטחה ומוכנות ההגנה של הענן של הארגון. (4 אותיות)

5 מאוזן: גיבוי יצירת עותקים מאובטחים מחוץ לאתר כדי לשחזר במקרה של כשלי מערכת. (5 אותיות)

6 מאוזן: פריצה אירוע אבטחה שבו נתונים מוגנים נגישים או נחשפים ללא הרשאה (5 אותיות)

8 מאוזן: מיסוך החלפת תווים רגישים בשדות מסד הנתונים כדי להגן על זהויות אישיות. (5 אותיות)

מאונך

1 מאונך: הצפנה הפיכת טקסט גלוי לטקסט מוצפן בלתי קריא כך שנתונים שנחטפו נשארים פרטיים (5 אותיות)

2 מאונך: צמצום הגבלת איסוף הנתונים האישיים למינימום ההכרחי לפעילות. (5 אותיות)

4 מאונך: גישה הגבלת הרשאות קריאה וכתיבה במסד הנתונים לתפקידי משתמש מאומתים. (4 אותיות)

7 מאונך: ציות עמידה בתקנים רגולטוריים כמו GDPR או CCPA בניהול מידע פרטי של משתמשים. (4 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. נפההצ — **הצפנה**
2. צסוצמ — **צמצום**
3. העדמ — **עמדה**
4. תוצי — **ציות**
5. ביגוי — **גיבוי**
6. שהגי — **גישה**
7. צהפיר — **פריצה**
8. רמסוי — **מיסוך**

מפתח אתגר הצופן הסודי

"הגנו על נתונים פרטיים בעזרת בקרות"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: שדרוג הצפנת מסד נתונים ארגוני במצב מנוחה

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: קמעונאי מקוון מאחסן מסדי נתוני עסקאות באחסון ענן ללא הצפנת דיסק מלאה. ביקורת תאימות אחרונה סימנה זאת כסיכון חמור לאבטחת נתונים לפי CCPA. תכננו ארכיטקטורת שחזור.
- אסטרטגיה ופתרון מומלצים: יישמו הצפנת דיסק מלאה AES-256 במנוחה בכל מערכות הקבצים. השתמשו בשירות ניהול מפתחות (KMS) מרכזי עם החלפה אוטומטית, ואכפו מדיניות IAM מחמירה לשליטה בגישה לפענוח.

B מקרה בוחן 2: בלימת כופרה ושחזור נתונים

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: התקפת תוכנת כופר פעילה מצפינה כונני רשת ברשת מקומית ארגונית. מנהל המערכת זיהה את ההדבקה בשלב מוקדם. תכננו את שלבי הבלימה וההתאוששות.
- אסטרטגיה ופתרון מומלצים: בודדו מיד את המקטע שנפגע. פרמטו את נקודות הקצה שנפגעו ושחזרו מהגיבוי האחרון במצב לא מקוון מסוג write-once-read-many (WORM). ודאו את תקינות הגיבוי לפני חיבור המערכות מחדש.