שם: _____ תאריך: _____ ציון: _____

יסודות אבטחת סייבר ואיומים ברשת מניעה

איומי סייבר, חומות אש ברשת, אימות רב-שלבי, מסגרות אבטחה

סקירת למידה: יסודות אבטחת סייבר

אובטח

הצפנת נתונים

תקן AES של 256 סיביות

תואם

תקנים עולמיים

מסגרות GDPR ו-CCPA

אפס אמון

מדיניות גישה

אימות רב-גורמי

ברוכים הבאים! חוברת הפעילויות הזו תדריך אתכם דרך העקרונות הבסיסיים של יסודות אבטחת הסייבר ומניעת איומים מקוונים. תחקרו איומי נוזקות, אימות רב-גורמי, חומות אש ברשת ומסגרות תגובה לאירועים.

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/

מפת הלמידה שלכם: יסודות אבטחת הסייבר

- זהו וקטורים נפוצים של נוזקות, פישינג ופריצה לרשת ארגונית.
- יישמו בקרות סייבר סטנדרטיות, כולל MFA, חומות אש והגנה על נקודות קצה.
- העריכו נהלי תגובה לאירועים להפחתת השפעות של דליפת נתונים.
- נתחו גורמי סיכון ארגוניים והתאמת אבטחה לפי הנחיות NIST.
- הגדירו נהלי היגיינת אבטחה כדי לצמצם התקפות Credential Stuffing אוטומטיות.

הוראות למדריך אבטחת סייבר

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 מניעת איומים. ולסיום, פעילות הבונוס "חשבו מהר".

יסודות אבטחת סייבר ומניעת איומים (מבוא)

אבטחת סייבר מגנה על רשתות, מערכות ונתונים מפני התקפות דיגיטליות לא מורשות. פיתוח הרגלי אבטחה חזקים, הגדרת חומות אש, דרישה לאימות רב-שלבי והדרכת צוות בזיהוי איומים הם מרכיבים חיוניים בהגנה על רשת ארגונית.

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. מהי המטרה העיקרית של התקפת פישינג?

- A. גניבת אישורי גישה ונתוני משתמש רגישים
- B. שיפור הנראות של האתר במנועי חיפוש
- C. הגדלת קיבולת רוחב הפס של הרשת
- D. ניהול שכפול גיבוי של מרכז נתונים

2. איזה מנגנון מספק את ההגנה החזקה ביותר על חשבון?

- A. אימות רב-גורמי באמצעות מפתחות חומרה
- B. סיסמאות מורכבות המתעדכנות כל שלושים יום
- C. הגבלת הכניסה לחשבון לשעות העסקים
- D. הסתרת שם המשתמש של החשבון מספריות ציבוריות

3. מה מגדיר את מטען ההדבקה של כופרה?

- A. הצפנת קובצי מערכת ודרישת תשלום
- B. רישום שקט של הקשות מקלדת בשרתים מרוחקים
- C. הזרקת פרסומות לא מורשות לדפדפנים
- D. שימוש במשאבי המעבד המקומי לכריית קריפטו

4. כיצד ניצול של פרצת יום-אפס משפיע על מנגנוני ההגנה?

- A. הוא מכוון לפגיעויות לא מתוקנות ולא מוכרות
- B. הוא משבית אוטומטית את חומת האש הארגונית
- C. הוא מאלץ את המערכת לבצע אתחול קשיח
- D. הוא אינו דורש תקציב כלל לתיקון

5. איזו מסגרת מסדירה בקרות אבטחה ארגוניות?

- A. הנחיות מסגרת אבטחת הסייבר של NIST
- B. מפרטי סכמת מסמכי HTML5 של W3C
- C. מדריכי התקנה של מנהלי התקן למדפסת
- D. הגדרות פרוטוקולי ניתוב של IETF

נקודת ביקורת 2: אתגר נכון או לא נכון

6 שאלה נכון/לא נכון 6

6. התקפות פישינג מכוונות רק לחשבונות דוא"ל אישיים.

○ נכון ○ לא נכון

7 שאלה נכון/לא נכון 7

7. אימות רב-שלבי עוזר לחסום התקפות credential stuffing.

○ נכון ○ לא נכון

8 שאלה נכון/לא נכון 8

8. חומות אש בודקות את תעבורת הרשת כדי לחסום גישה לא מורשית לפורטים.

○ נכון ○ לא נכון

9 שאלה נכון/לא נכון 9

9. תיקון ניצולי zero-day מחייב עדכוני הגדרות אנטי-וירוס רגילים.

○ נכון ○ לא נכון

10 שאלה נכון/לא נכון 10

10. honeypot הוא שרת פיתיון המשמש לפתות פושעי סייבר.

○ נכון ○ לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. מנהלי רשת מתקינים _____ כדי לסנן תעבורה נכנסת.
2. תוקף מפעיל _____ ליום אפס כדי לעקוף תיקוני מערכת.
3. תוקפים שולחים הודעות דואר אלקטרוני מזויפות כדי לנהל קמפייני _____ נגד עובדים.
4. תוכנת כופר היא סוג הרסני של _____ שנועלת נתוני משתמשים.
5. הקפדה על _____ בניהול סיסמאות מצמצמת את הסיכון לגניבת פרטי זיהוי.
6. כדי להגן על תקשורת רגישה, משתמשים מפעילים פרוטוקולי _____ .

בנק מילים

היגיינה | הצפנה | חומת אש | מסגרת | נוזקה | ניצול חולשה | פישינג | רב גורמי

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים באבטחה

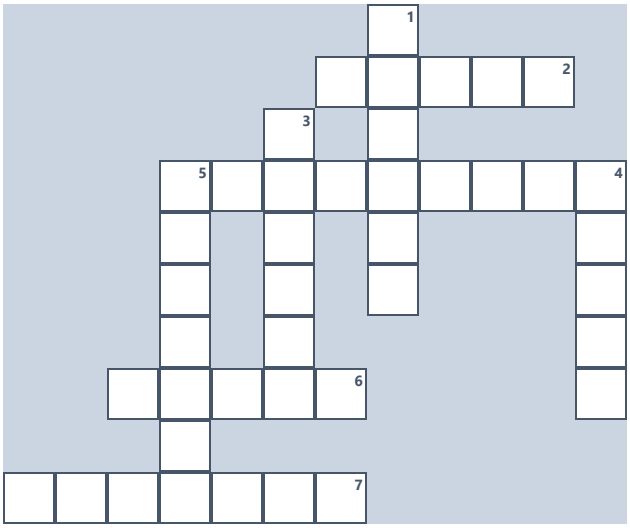
התאמת הגדרות

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

1. איום כופרה	A	הנחיות מובנות כמו NIST המשמשות לניהול סיכוני סייבר.
2. אימות רב-גורמי	B	תוכנית מובנית לטיפול בפרצות אבטחה ולצמצום השפעתן.
3. ניצול אפס-יום	C	מחסום רשת המסנן תעבורה לפי כללי אבטחה.
4. פיתיון דבש	D	נוזקה המצפינה נתונים ודורשת תשלום כספי עבור פענוחם.
5. חומת אש נגד חדירות	E	ניצול פרצה המכוון לפני שהספק פרסם תיקון.
6. תגובה לאירועים	F	שיטות עבודה מומלצות לניהול פרטי גישה ומפתחות אימות.
7. היגיינת סיסמאות	G	אימות אבטחה הדורש שני גורמי אימות או יותר.
8. מסגרת אבטחה	H	מערכת פיתיון שמוקמת כדי למשוך תוקפים זדוניים ולנתח אותם.

נקודת ביקורת 5: תשבץ

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



מאוזן

2. מערכת מלכודת שמוקמת כדי למשוך גורמים זדוניים ולנתח אותם (5)

4. נוזקה שמצפינה נתונים ודורשת תשלום כספי עבור פענוחם (9)

6. הנחיות מובנות כמו NIST המשמשות לניהול סיכוני סייבר (5)

7. שיטות עבודה מומלצות לניהול פרטי זיהוי ומפתחות אימות (7)

מאונך

1. מחסום רשת שמסנן תעבורה לפי כללי אבטחה (6)

3. ניצול חולשה שמכוון אליה לפני שיצא תיקון מהיצרן (6)

4. תוכנית מובנית לטיפול בפרצות אבטחה ולצמצום נזקיהן (5)

5. אימות אבטחה שמחייב שני גורמי הזדהות או יותר (7)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

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

מאוזן

2 מאוזן: מערכת מלכודת שמוקמת כדי למשוך גורמים זדוניים ולנתח אותם (5 אותיות):

4 מאוזן: נוזקה שמצפינה נתונים ודורשת תשלום כספי עבור פענוחם (9 אותיות):

6 מאוזן: הנחיות מובנות כמו NIST המשמשות לניהול סיכוני סייבר (5 אותיות):

7 מאוזן: שיטות עבודה מומלצות לניהול פרטי זיהוי ומפתחות אימות (7 אותיות):

מאונך

1 מאונך: מחסום רשת שמסנן תעבורה לפי כללי אבטחה (6 אותיות):

3 מאונך: ניצול חולשה שמכוון אליה לפני שיצא תיקון מהיצרן (6 אותיות):

4 מאונך: תוכנית מובנית לטיפול בפרצות אבטחה ולצמצום נזקיהן (5 אותיות):

5 מאונך: אימות אבטחה שמחייב שני גורמי הזדהות או יותר (7 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

רשימת מילים

תוכנתכופר | רבגורמי | יוסאפס | פתיון | חומתאש | תגובה | היגיינה | מסגרת

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. תוכנתכופר
B. רבגורמי
C. יומאפס
D. פתיון
E. חומתאש
F. תגובה
G. היגיינה
H. מסגרת

הגדרות ושדות התאמה	
1. מחסום רשת שמסנן תעבורה לפי כללי אבטחה.	
2. תוכנית מובנית לטיפול בפרצות אבטחה ולצמצום נזקיהן.	
3. נוזקה שמצפינה נתונים ודורשת תשלום כספי עבור פענוחם.	
4. אימות אבטחה שמחייב שני גורמי הזדהות או יותר.	
5. שיטות עבודה מומלצות לניהול פרטי זיהוי ומפתחות אימות.	
6. הנחיות מובנות כמו NIST המשמשות לניהול סיכוני סייבר.	
7. ניצול חולשה שמכוון אליה לפני שיצא תיקון מהיצרן.	
8. מערכת מלכודת שמוקמת כדי למשוך גורמים זדוניים ולנתח אותם.	

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. כתנותופרכ
2. סיספאו
3. חמתשאו
4. הייינהג
5. ריוגרמב
6. ופיות
7. בהתוג
8. תמגרס

פעילות בונוס: חשבו מהר

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

1	משרות באבטחת סייבר		
2	סיבות לעדכן תוכנה		
3	דברים שחומת אש יכולה לחסום		
4	סימני אזהרה באימייל		
5	דברים שמגבים		
6	סוגים מוכרים של התקפות סייבר		
7	דברים שפיתיון דבש (honeypot) יכול לפתות		
8	מידע שלעולם אסור לשתף		
9	סימנים לכך שמחשב נדבק		
10	סרטים או סדרות על האקרים		
11	שכבות אבטחה שאפשר לבנות		
12	דברים לתרגל בתרגיל אבטחה		
13	כלי אבטחה שאתם מכירים		
14	אנשים שאפשר לבקש מהם עזרה ב-IT		
15	מילים שמתחילות ב"סייבר"		

נקודת ביקורת 8: מקרי בוחן באבטחת סייבר

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

מקרה בוחן 1: אסטרטגיית התאוששות מכופרה

👨‍💻

תרחיש: רשת ארגונית נדבקה בתוכנת כופר שנועלת מסדי נתונים קריטיים. התוקפים דורשים תשלום של 100,000 דולר במטבע קריפטוגרפי. לחברה יש גיבויים לא מקוונים מלפני 24 שעות.

שאלה לדיון: נתחו את הסיכונים בתשלום, והעריכו את אסטרטגיית ההתאוששות.

מקרה בוחן 2: הגנות מפני Credential Stuffing

👨‍💻

תרחיש: שירות מקוון חווה התקפת credential stuffing, שבה האקרים בודקים מיליוני צמדי שם משתמש/סיסמה שנגנבו מאתרים אחרים.

שאלה לדיון: פרטו את מנגנון ההתקפה הזו, ותארו בקצרה שתי מערכות הגנה.

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

22	20	7	16	2	22	11	20	16	13	6	8	9	2	1

10	13	20	6	3	2	20	22	6	13	10	1

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 המטרה העיקרית של אבטחת סייבר?

המטרה העיקרית היא הגנה על רשתות, מכשירים ונתונים מפני גישה לא מורשית, התקפות ונזק מקרי.

Q2: במה פישינג שונה מפישינג ממוקד (spear phishing)?

פישינג הוא קמפיין דוא"ל רחב המכוון למשתמשים אקראיים, ואילו פישינג ממוקד (spear phishing) מכוון לאנשים מסוימים באמצעות נתונים מותאמים אישית.

Q3: מהי חומת אש לרשת?

חומת אש היא מערכת אבטחת רשת שמנטרת ומסננת תעבורה נכנסת ויוצאת על בסיס כללי אבטחה שהוגדרו מראש.

Q4: מדוע אימות רב-שלבי (MFA) הכרחי?

MFA מוסיף שכבת הגנה קריטית ומונע גישה גם אם תוקפים גונבים או פורצים את פרטי הסיסמה הראשית.

Q5: מה מגדיר וירוס מחשב?

וירוס הוא נוזקה משכפלת עצמה שמתחברת לקבצים תקינים ומתפשטת במערכות לאחר שהופעלה.

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

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q6: כיצד תוכנת כופר נועלת נתונים מקומיים?

תוכנת כופר משתמשת באלגוריתמים קריפטוגרפיים להצפנת קבצי המשתמש, ובכך הופכת אותם לבלתי קריאים עד להחלת מפתח פענוח.

Q7: מהי פגיעות zero-day?

zero-day הוא פגם אבטחה בתוכנה שאינו ידוע ליצרן, כך שלא נותר זמן לפיתוח תיקון לפני ניצולו.

Q8: מה תפקידה של מסגרת NIST?

מסגרת NIST מספקת הנחיות ותקנים וולונטריים שנועדו לסייע לארגונים לנהל ולהפחית סיכוני אבטחת סייבר.

Q9: מהי תוכנית תגובה לאירועי אבטחה?

זהו סט מתועד של נהלים לזיהוי, בלימה והתאוששות מפריצות אבטחה ופגיעה ברשת.

Q10: כיצד הנדסה חברתית מנצלת משתמשים?

הנדסה חברתית משתמשת במניפולציה פסיכולוגית כדי להערים על עובדים לחשוף סיסמאות או להוריד קבצים זדוניים.

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

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

Q1: כיצד התקפת DDoS מציפה שרתי אינטרנט?

התקפת DDoS מתאמת מיליוני מכשירי בוטנט שנפרצו כדי להציף שרת בתעבורה ולנצל עד תום את מגבלות רוחב הפס והמעבד.

Q2: מה ההבדל בין הצפנה סימטרית לא-סימטרית?

הצפנה סימטרית משתמשת במפתח יחיד להצפנה ולפענוח, ואילו הצפנה אסימטרית משתמשת בזוג מפתחות ציבורי ופרטי.

Q3: כיצד האקרים מבצעים התקפות הזרקת SQL?

תוקפים מזינים פקודות SQL זדוניות לשדות בטפסים ומטעים את מסד הנתונים האחורי למסור רשומות משתמשים ללא הרשאה.

Q4: מהי תנועה רוחבית (lateral movement) בפריצות לרשת?

זוהי טכניקה שבה תוקפים מנצלים גישה ראשונית לשרת כדי לפגוע במערכות מקושרות אחרות ברשת הפנימית.

Q5: כיצד זיוף DNS מפנה תעבורת אינטרנט?

זיוף DNS משנה רשומות במטמון של שרת שמות ומנתב משתמשים לגיטימיים לאתרים זדוניים דומים במקום לדומיינים המיועדים.

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

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

Q6: מהו אסימון אבטחה חומרתי?

זהו התקן פיזי (כמו YubiKey) שמפיק הוכחות אימות קריפטוגרפיות ומציע הגנה מרבית מפני פישינג מרחוק.

Q7: כיצד צוותי אבטחה משתמשים בפיתיונות honeypot?

צוותים מפעילים שרתי פיתיון שאינם בסביבת ייצור כדי לזהות חדירות מוקדם ולנתח את דפוסי התקיפה של גורמים לא מורשים.

Q8: מהו עקרון ההרשאה המינימלית?

זהו תקן אבטחה של הגבלת זכויות הגישה של משתמשים למינימום ההכרחי לביצוע תפקידי העבודה שלהם.

Q9: כיצד התקפת אדם-באמצע (Man-in-the-Middle) מנצלת חיבורים?

תוקף מיירט ומשנה תקשורת בין שני מכשירים ברשתות לא מוצפנות, וגונב אסימוני הפעלה ואישורי גישה.

Q10: מהם אינדיקטורים לפריצה (IOCs)?

IOCs הם רמזים משפטיים-דיגיטליים, כמו שינויים חריגים ברישום המערכת או תעבורת IP זדונית, שמראים שמערכת נפרצה.

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

תוקפים סורקים את האינטרנט ללא הרף בחיפוש אחר שרתים פגיעים ושולחים הודעות פישינג לתיבות הדואר של עובדים.

2. תובנות על אבטחה

טעות אנוש, כמו לחיצה על קישורי פישינג, היא גורם נפוץ בפריצות נתונים, ולכן הדרכה חשובה.

3. תובנות על אבטחה

עלויות של דליפת נתונים כוללות קנסות משפטיים, אובדן לקוחות, חקירה ותיקון, ויכולות להגיע למיליוני דולרים.

4. תובנות על אבטחה

אימות רב-שלבי עמיד בפני פישינג, כגון מפתחות אבטחה פיזיים, הוא סוג ה-MFA החזק ביותר והתקן ש-CISA מעודדת. [2]

5. תובנות על אבטחה

תוכנת כופר נותרת איום מרכזי על רשתות ארגוניות, ו-CISA מעודדת גיבויים מוצפנים ולא מקוונים כהגנה מרכזית. [4]

6. תובנות על אבטחה

למסגרת אבטחת הסייבר של NIST גרסה 2.0 (2024) יש שש פונקציות ליבה: ממשל, זיהוי, הגנה, איתור, תגובה והתאוששות. [1]

7. תובנה על אבטחה

בוטים של Credential Stuffing בודקים בקנה מידה גדול זוגות שם משתמש וסיסמה שדלפו מול פורטלי כניסה של בנקים ושל מסחר אלקטרוני.

8. תובנה על אבטחה

קיימים שווקים של ניצולי יום אפס ברחבי העולם, שבהם פגיעויות בחומרה גבוהה יכולות להימכר בסכומים גדולים לפני שהן מתוקנות.

9. תובנה על אבטחה

מערכת פיתיון מסוג honeypot מדווחת מיד על התראות חדירה, משום שלמשתמשים לגיטימיים אין סיבה לגשת אליה.

10. תובנות על אבטחה

Transport Layer Security (TLS) מצפין הפעלות דפדפן ומונע האזנה למנות ברשתות Wi-Fi ציבוריות.

מקורות והפניות טכניים

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

מקורות אקדמיים ותעשייתיים

[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

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 התקפות פישינג

פישינג

תשובה נכונה: A

הערה למורה

קמפייני פישינג מנסים לגנוב פרטי גישה ונתוני משתמש רגישים באמצעות הודעות דוא״ל מזויפות. מקור: OWASP Secure Configuration.

2 הגנת חשבון

מפתח MFA

תשובה נכונה: A

הערה למורה

אימות רב-גורמי (MFA) באמצעות אסימוני חומרה מספק את ההגנה החזקה ביותר על הגישה לחשבון. ציטוט: NIST Digital Identity.

3 איום תוכנת כופר

תוכנת כופר

תשובה נכונה: A

הערה למורה

תוכנת כופר מצפינה מערכות ונתונים קריטיים ודורשת תשלום במטבע קריפטוגרפי תמורת מפתחות פענוח. מקור: Center for Internet Security (CIS).

4 פגיעות יום אפס

יום אפס

תשובה נכונה: A

הערה למורה

איומי יום אפס מנצלים פגמי אבטחה לא מתוקנים ולא ידועים לפני שזמין תיקון מהספק. ציטוט: OWASP Secure Configuration.

5 מסגרות אבטחה

מסגרות

תשובה נכונה: A

הערה למורה

מסגרות כמו NIST מספקות הנחיות מובנות שעוזרות לארגונים לנהל ולצמצם סיכוני סייבר. מקור: NIST Digital Identity.

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 **פישינג ממוקד** פישינג **תשובה נכונה: לא נכון**

הערה למורה

התקפות פישינג מכוונות הן לרשתות ארגוניות והן לחשבונות אישיים כדי להרחיב את וקטורי הניצול. מקור: OWASP Secure Configuration.

7 **שאלה 7** **תשובה נכונה: נכון**

הערה למורה

אימות רב-שלבי דורש גורם שני, ולכן סיסמה גנובה לבדה אינה מספיקה בדרך כלל כדי להתחבר.

8 **חומת אש לתעבורה** חומת אש **תשובה נכונה: נכון**

הערה למורה

חומות אש בודקות וחוסמות תעבורה בפורטים מסוימים ברשת כדי לסנן חיבורים לא מורשים. מקור: Center for Internet Security (CIS).

9 **תגובה ליום אפס** יום אפס **תשובה נכונה: לא נכון**

הערה למורה

תיקון פגיעויות zero-day מחייב טלאי קוד וסינון WAF, כי עדיין אין חתימות. מקור: OWASP Secure Configuration.

10 **פתיונות דמה (Honeypots)** מלכודת דבש **תשובה נכונה: נכון**

הערה למורה

Honeypots הם שרתים מתעתעים שצוותי אבטחה משתמשים בהם כדי לפתות, להתריע ולחקור גורמים זדוניים. מקור: Center for Internet Security (CIS).

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

D 1. איום כופרה	G 2. אימות רב-גורמי	E 3. ניצול אפס-יום	H 4. פיתיון דבש
C 5. חומת אש נגד חדירות	B 6. תגובה לאירועים	F 7. היגיינת סיסמאות	A 8. מסגרת אבטחה

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 חומת אש	2 ניצול חולשה	3 פישינג	4 נוזקה
5 היגיינה	6 הצפנה		

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

1 E – חומתאש	2 F – תגובה	3 A – תוכנתכופר	4 B – רבגורמי
5 G – היגיינה	6 H – מסגרת	7 C – יומאפס	8 D – פתיון

הערות לדיון עבור מורים

מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את איום כופרה, אימות רב-גורמי ו-ניצול אפס-יום 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.

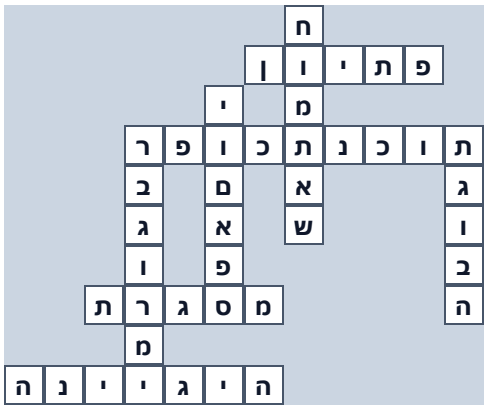
מפתחות פאזלים והערות למורה

פתרון תפזורת

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

פתרון תשבץ

							ח							
						ן	ו	י	ת	פ				
					י		מ							
			ר	פ	ו	כ	ת	נ	כ	ו	ת			
			ב		ם		א				ג			
			ג		א		ש				ו			
			ו		פ						ב			
		ת	ר	ג	ס	מ					ה			
			מ											
ה	נ	י	י	ג	י	ה								



מדריך למורה לפתרונות התשבץ

מאוזן

2 מאוזן: פתיון מערכת מלכודת שמוקמת כדי למשוך גורמים זדוניים ולנתח אותם (5 אותיות)

4 מאוזן: תוכנתכופר נוזקה שמצפינה נתונים ודורשת תשלום כספי עבור פענוחם (9 אותיות)

6 מאוזן: מסגרת הנחיות מובנות כמו NIST המשמשות לניהול סיכוני סייבר (5 אותיות)

7 מאוזן: היגיינה שיטות עבודה מומלצות לניהול פרטי זיהוי ומפתחות אימות (7 אותיות)

מאונך

1 מאונך: חומתאש מחסום רשת שמסנן תעבורה לפי כללי אבטחה (6 אותיות)

3 מאונך: יומאפס ניצול חולשה שמכוון אליה לפני שיצא תיקון מהיצרן (6 אותיות)

4 מאונך: תגובה תוכנית מובנית לטיפול בפרצות אבטחה ולצמצום נזקיהן (5 אותיות)

5 מאונך: רבגורמי אימות אבטחה שמחייב שני גורמי הזדהות או יותר (7 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. כתנותופרכ — **תוכנתכופר**
2. סיספאו — **יוסאפס**
3. חמתשאו — **חומתאש**
4. הייינהג — **היגיינה**
5. ריוגרמב — **רבגורמי**
6. ופיקת — **פתיון**
7. בהתוג — **תגובה**
8. תמגרס — **מסגרת**

מפתח אתגר הצופן הסודי

"אבטחו מערכת בעזרת אימות רב גורמי"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: אסטרטגיית התאוששות מכופרה

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: רשת ארגונית נדבקה בתוכנת כופר שנעלה מסדי נתונים קריטיים. התוקפים דורשים תשלום של 100,000$ במטבע קריפטוגרפי. לחברה יש גיבויים לא מקוונים מלפני 24 שעות.
- אסטרטגיה ופתרון מומלצים: סיכוני תשלום: תשלום אינו מבטיח פענוח קבצים, מסמן את החברה כיעד שמשלם וממן פעילות פושעת. אסטרטגיית התאוששות: על הצוות לבודד מארחים נגועים, למחוק שרתים שנפגעו ולשחזר נתונים מגיבויים לא מקוונים. עליו לתקן את וקטור הגישה הראשוני (פישינג או ניצול חולשה) כדי למנוע הדבקה חוזרת מיידית.

B מקרה בוחן 2: הגנות מפני Credential Stuffing

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: שירות מקוון חווה מתקפת credential stuffing, שבה האקרים בודקים מיליוני צמדי שם משתמש וסיסמה שנגנבו מאתרים אחרים.
- אסטרטגיה ופתרון מומלצים: מנגנון: תוקפים מנצלים שימוש חוזר בסיסמאות באתרים שונים, באמצעות בוטים אוטומטיים, כדי להיכנס לחשבונות משתמשים. הגנות: 1. אימות רב-שלבי (MFA) חוסם ניסיונות התחברות גם אם הסיסמה נכונה. 2. הגבלת קצב (rate-limiting) ו-CAPTCHA חוסמות תעבורת בוטים אוטומטית מהצפת נקודות הקצה של ההתחברות.