

המכללה האקדמית תל אביב יפו
בית הספר לכלכלה וניהול
החוג למערכות מידע

אבטחת מידע ממוחשב, 272012

ד"ר טל פבל

תשע"ח, סמסטר א', מועד א', 19/02/2018

--	--	--	--	--	--	--	--	--

מספר זהות

משך הבחינה: שעתיים

ללא חומר עזר

בבחינה 25 שאלות, יש לענות על כולן. משקל השאלות זהה - 4 נקודות לשאלה.
בכל שאלה יש לסמן את התשובה הנכונה (אחת בלבד), באופן ברור, בדף התשובות בלבד. אם סימנת יותר מתשובה אחת - השאלה תיפסל!
יתקבלו תשובות שנכתבו על גבי דף התשובות בלבד. לא ייבדקו תשובות שלא ייכתבו בדף המיועד לכך.

סימון תשובות בטופס הבחינה לא יהווה בסיס לערעור.

יש להחזיר את דף התשובות ביחד עם טופס הבחינה, אחרת הבחינה לא תיבדק.

**נא לשים לב כי דף התשובות מוכן לטופס בחינה של 6 תשובות. בבחינה זו יש 4 תשובות לכל היותר.
יש להקפיד למלא את התשובות במקום הנכון!**

בהצלחה!

שאלה מספר 1:

מהי סטגנוגרפיה?

- א. הסתרת קיומו של המידע
- ב. הסתרת תוכנו של המידע
- ג. הסתרת שולח המידע
- ד. הסתרת מקבל המידע

שאלה מספר 2:

מה מגדיר מודל ה-CIA?

- א. הצורך כי המידע יהיה סודי, שלם וזמין
- ב. הצורך לשילוב אופטימלי בין טכנולוגיות, אנשים ותהליכים
- ג. חלוקת העבודה האופטימלית בין דירקטוריון, הנהלה בכירה ומנהל אבטחת מידע
- ד. חלק ממדדי האבטחה היעילים לבחינת פעילות הארגון בתחום אבטחת המידע

שאלה מספר 3:

למה מתייחסת ההגדרה "שינוי חומרה ותוכנה של מחשב על מנת להשיג מטרה השונה מהמטרה המקורית של המערכת"?

- א. Hacking
- ב. DDoS
- ג. Phishing
- ד. Defacement

שאלה מספר 4:

מה ניתן לומר על **DRP** – תוכנית התאוששות מאסון?

- א. תשובות ב' ו - ג' נכונות
- ב. מתייחס לסיכונים למערכות המידע של הארגון
- ג. מהווה חלק מה-BCP
- ד. תוכנית כוללת שנועדה לצמצם את הסיכונים במקרה של שיבוש בתחומי פעילות קריטיים של הארגון

שאלה מספר 5:

מה מטרת הקריפטוגרפיה?

- א. כל התשובות נכונות
- ב. יצירת תקשורת מאובטחת
- ג. שמירה על פרטיות
- ד. שמירה על אותנטיות המידע

שאלה מספר 6:

מיהו **Craker** (פרצן)?

- א. תשובות ב' ו - ד' נכונות
- ב. הגרסה הפלילית של האקר
- ג. הגרסה החוקית של האקר
- ד. אדם הפועל ממניעים של רווח, מחאה, איסוף מודיעין ואתגר

שאלה מספר 7:

מה מתארת ההגדרה "הגנה ושימור המידע. הגנה ושימור הסודיות, השלמות, המקוריות, הזמינות והאמינות של המידע"?

- א. אבטחת מידע
- ב. הבטחת מידע
- ג. משילות אבטחת המידע
- ד. סטגנוגרפיה

שאלה מספר 8:

מה ההבדל בין אבטחת מידע לבין הבטחת מידע?

- א. אבטחת מידע מהווה הכלים והטקטיקות ומהווה חלק מהבטחת המידע העוסקת בהיבטים אסטרטגיים יותר
- ב. הבטחת מידע עוסקת בטכנולוגיה ובתפעול לעומת אבטחת מידע העוסקת בהגנה על המידע הקריטי בצורה יעילה יותר
- ג. אבטחת מידע מהווה הדרך לניהול סיכונים הקשורים במידע, בעוד הבטחת מידע מהווה הדרך להגנת המידע ומערכות המידע מפעילות בלתי מורשית
- ד. תשובות ב' ו - ג' נכונות

שאלה מספר 9:**מה ההבדל העיקרי בין DoS לבין DDoS?**

- א. מספר התוקפים
- ב. סוג המתקפה המבוצעת
- ג. סוג היעד המותקף
- ד. זהות התוקפים

שאלה מספר 10:**מהו Plaintext?**

- א. המידע הגלוי
- ב. המידע המוצפן
- ג. מפתח ההצפנה הידוע רק לשולח ולמקבל
- ד. אלגוריתם ההצפנה

שאלה מספר 11:**מה הוא Substitution Cipher?**

- א. שיטת הצפנה המבוצעת על ידי החלפת יחידות של מידע גלוי במוצפן על פי שיטה רגילה
- ב. שיטת הצפנה בה מיקום יחידות המידע הגלוי מוזז בהתאם לשיטה רגילה
- ג. שיטת הצפנה מכנית המבוססת רוטור
- ד. שיטת הצפנה ממוחשבת המבוססת אלגוריתם

שאלה מספר 12:**מה ניתן לומר על Defacement?**

- א. התקפה אשר משמשת במקרים רבים במה להפצת מסר מצד ארגוני טרור והאקטיביסטים, אך גם מצד האקרים חובבים לפרסום שמם ופעילותם
- ב. אמצעי גישה למערכות מחשב או למידע מוצפן העוקף את מנגנוני ההגנה המקובלים
- ג. מבוצעת תוך התחזות לגורם אמין ולגיטימי באמצעות משלוח הודעות המעוררות סקרנות או פחד לשם הנעת הקורבן לפעולה
- ד. מתקפה המכוונת לשינוי או חבורת ממוקדות

שאלה מספר 13:**מהי משילות בתחום מערכות המידע?**

- א. כל התשובות נכונות
- ב. מספקת כיוון אסטרטגי לפעולות האבטחה
- ג. מוודאת כי סיכוני אבטחת המידע מנוהלים כראוי
- ד. מסייעת להבטיח כי משאבי המידע משמשים בצורה אחראית

שאלה מספר 14:**מה תפקיד הדיקטוריון וההנהלה הבכירה?**

- א. אחראים על הגדרת משילות אבטחת המידע
- ב. אחראים על מימוש משילות אבטחת מידע בצורה יעילה והגדרות יעדי האבטחה האסטרטגיים
- ג. אחראים לוודא את מעורבות כל בעלי העניין המושפעים משיקולי האבטחה
- ד. מהווים ערוץ תקשורת יעיל המספק בסיס מתמשך להבטחת התאמת תוכנית האבטחה עם היעדים העסקיים

שאלה מספר 15:**איזו רמה מאפיינת פעילות של סיווג המידע והמשתמש, וכן יצירת הרשאות?**

- א. אבטחה ברמת המשתמש
- ב. אבטחת ברמת האפליקציה
- ג. אבטחת ברמת המערכות
- ד. אבטחה ברמת התשתית

שאלה מספר 16:**מהו "נכס" עבור הארגון?**

- א. כל דבר בעל ערך לארגון, לפעילותו העסקית ולהמשכיותו
- ב. מידע "טהור"
- ג. נכסים פיזיים
- ד. קניין רוחני ותוכנות

שאלה מספר 17:**באיזה סוג של הצפנה משתמשים בהחלפה של אות מקור באות הנמצאת בהיסט קבוע באלף בית?**

- א. צופן קיסר
- ב. צופן אתבש
- ג. צופן Pigpen
- ד. מכונת אניגמה

שאלה מספר 18:**מה מטרתו של איום על נכסי הארגון?**

- א. כל התשובות נכונות
- ב. האיום ינצל חולשה לשם פגיעה בבטחון של המידע, הנכס.
- ג. אובייקט, אדם או ישות אחרת המהווה איום מתמשך על הנכס
- ד. האיום יכול להיות פיזי, אסון טבע, כשלון טכני, חשיפה של מידע או של פונקציונאליות, אובדן שרותים הכרחיים

שאלה מספר 19:**מה מייחד את ההצפנה באניגמה?**

- א. הצפנת מכונה להבדיל מהצפנה המבוססת על ונייר
- ב. תחילת ההצפנה המבוססת על אלגוריתמים
- ג. הצפנה לשם שעשוע על ידי יצירת מילה או משפט חדשים באמצעות שיכול אותיות
- ד. שיטת הצפנה מהעת העתיקה אשר נדרשו 800 שנה לפצח אותה

שאלה מספר 20:**מה מגדיר בצורה הטובה ביותר "סיכון"?**

- א. הפוטנציאל שאיום נתון ינצל פגיעויות בנכס או בקבוצת נכסים ויגרום נזק לארגון
- ב. התוצאה של ארוע אבטחת מידע, אשר נגרם בשל איום אשר השפיע על הנכס
- ג. נזק למוניטין ולמיתוג ונאמנות הלקוחות
- ד. אדם או קבוצה היכולים להוות איום על נכסי הארגון

שאלה מספר 21:**מהו הערך של ה"נכס" לארגון?**

- א. כל התשובות נכונות
- ב. הערך של הנכס למתחרה
- ג. עלות ההתאוששות או השחזור
- ד. הנזק לפעולות אחרות

שאלה מספר 22:**מה ההבדל בין הצפנה סימטרית להצפנה א-סימטרית?**

- א. בהצפנה א-סימטרית אין צורך להעביר את מפתח ההצפנה בצורה סודית וניתן לפרסמו פומבית
- ב. בהצפנה א-סימטרית המפתח הוא סודי אבל יש לשתף את כל המפתח באמצעות הסדר מקדים
- ג. בהצפנה סימטרית אין צורך להעביר את מפתח ההצפנה בצורה סודית וניתן לפרסמו פומבית
- ד. בהצפנה א-סימטרית שיטת ההצפנה והפענוח היא זהה

שאלה מספר 23:**למה מהווים דוגמא האקרים, פושעים, מתחרים, משתמשים מתוחכמים, האקטיביסטים?**

- א. Threat Agent
- ב. Vulnerability
- ג. Risk
- ד. Impact

שאלה מספר 24:**בתוך מה נכללים הרכיבים; Security Countermeasures, Security Services, Information States?**

- א. Information Assurance
- ב. Information Security
- ג. Policies and Practices
- ד. People and Technology

שאלה מספר 25:**מה מטרתו של ה-Threat Agent?**

- א. תשובות ב' ו - ג' נכונות
- ב. לחפש גישה לנכס הארגוני
- ג. למנף איומים קיימים היכולים לנצל פגיעויות
- ד. להפחית את הסיכון על נכסי הארגון

--- סוף המבחן ---