**מבוא לאבטחת סייבר – מושגים מההרצאות**

**סגמנטציה** – חלוקה לאזורים לפי רמות אבטחה

**DMZ**- אזור מפורז, יהיו בו דברים שלא צריכים הצפנה

**Backdoor** – קיצור דרך שמפתחים משתמשים בו כדי לדלג על שלבי הזדהות ולהגיע לקוד העיקרי. מהווה פירצת אבטחה משמעותית – האקרים מחפשים פרצות כאלה.

**Security vs. usability** – קונפליקט תמידי.

**C.I.A –** בטיחות\סודיות, שלמות וזמינות.

**DOS –** מניעת שירות- תקיפת שרת בבקשות רבות מאשר הוא מוכן לקלוט, ובכך גרימה לקריסת השרת.

**DDOS –** מניעת שירות על ידי מספר גדול מאוד של בקשות באופן אוטומטי.

**בקרות / סיכונים** – אין צורך לשים בקרה כאשר אין סיכון – בזבוז כסף ומשאבים.

- אבטחת מידע מורכבת מ3 חלקים: טכנולוגיה, תהליכים ואנשים  
- חלוקת אחריות בארגון  
- משהו שאתה יודע, משהו שיש לך, משהו פיזי שלך (טביעת אצבע לדוגמה)

**Least premissions –** כמה שפחות הרשאות למשתמשים.

**וירוס –** תוקף מחשב יחיד

**תולעת –** וירוס שמדביק גם מחשבים אחרים

**APT** – מתקפה שדורשת הרבה משאבים – הכשרת אנשים וכדומה

**IRT** – צוות טיפול באירוע

**DRP** – תוכנית התאוששות מאסון – גיבוי מערכות הארגון באתר מרוחק מאתר הארגון (תשתית פיזית)

**BCP –** תוכנית המשכיות של העסק (מבחינת התנהלות עסקית)

**IAAA –** זיהוי, אימות, הרשאות, אחריותיות

**MFA –** multi factor authentication

**OTP –** one time password

**ISO27000** – תקן בינלאומי לאבטחת מידע, כמו כן קיים **NIST**, שהוא תקן אמריקאי מחמיר יותר לאבטחת מידע

**שכבות הגנה –** דורש סגמנטציה

**GDPR** – חוק הגנת הפרטיות האירופאי- מאי 2018

**Compliance** – עמידה בתקנים ורגולציות, מהווה סיכון ולכן יש החלטות איך לפעול

**סיכון –** מורכב ממכפלה של הסיכוי שיקרה נזק בסכום הנזק

**סיכון שיורי –** לאחר בדיקת הסיכון והקמת בקרות – זהו הסיכון שנשאר (אי אפשר למנוע סיכון לגמרי)

**מטרת אבטחת סייבר –** הבאת תיאבון הסיכון לרמת הסיכון השיעורי

**התמודדות עם סיכונים:**

1. **הפחתת סיכון (בקרות)**
2. **קבלת הסיכון**
3. **העברת סיכון – ביטוח**
4. **הימנעות מסיכון**

**בקרת גישה –** הסיכון- גישה של אדם לא מורשה

**MAC –** אין גימישות ושיקול דעת למשתמש בנוגע לגישה שלו למידע או למערכות. (מוגדר מראש)

**DAC –** מאפשר שינויים במתן גישה למשתמשים מסויימים

**Subject** – מי שפונה למערכת לקבלת מידע

**Objects –** המערכות אליהן ניגשים

**False Positive** – טעות כשלא אפשרתי למישהו שמותר לו להיכנס למערכת להיכנס אליה

**False Negative** – טעות כשאיפשרתי למי שאסור לו להיכנס למערכת להיכנס אליה

**Radius –** מערכת בקרת גישה מרחוק

**SSO –** single sign on

**IPS –** מניעת חדירה

**IDS –** זיהוי חדירה – חיפוש התנהגות חריגה

-ניתן להתקין IPDS על הרשת עצמה – לניטור הפאקטים שמגיעים לרשת ויוצאים מהרשת. ניתן גם להתקין על תחנות הקצה עצמן.

**מלכודת דבש –** זיהוי והרחקת התנהגות שונה במערכת לאזור מופרד ברשת.

**DLP –** הגנת זליגת מידע

**Non repudiation –** אי הכחשה

**הגנה מינימלית –** הגנה על השכבה הפיזית

**Zero day –** פגיעות ביישום שעדיין לא נכתב לה תיקון

**Exploit –** ניצול של הפריצה

**חשיבות עדכונים – קריטי לחומרה ולמערכות הפעלה.**

**אחריות על מערכות מידע בארגון – מנכ"ל (בפועל- CISO)**

**הסמכות:** CISSP, SANS, CISM

**קרברוס:** שלושה ראשים שרת אימות שמחלק הרשאת כניסה על ידי בדיקת המבקש  
**פרוקסי:** מיופה כוח  
 **:ACL**רשימת בקרת גישה

**:PCI** תקן לחברות שמשתמשות בסליקת אשראי

**-Least privilages –** נותן רק מה שביקשו

**-Need to know –** יודע מה הם הרשאות היוזר ואיזה מידע הוא צריך לדעת

**-מחזור החיים של מידע –** סיווג מידע 🡨 שימוש במידע 🡨 השמדת מידע

שאלות מהמבחן –

1. בארגון תומכים בדרך שכל עובד צריך גישה רק לנתונים עליהם הוא עובד במשימה מסויימת. הם עובדים בשיטה של: need to know
2. אדמין נותן גישה למסד נתונים. מהי ברירת המחדל שהוא יתן ליוזר חדש? 🡨 ללא גישה
3. למה חלוקת אחראיות חשובה לצרכי אבטחה? 🡨 מונע מאנשים שלא מורשים לבצע שינויים
4. מה היתרון של חלוקת אחראיות 🡨 מניעת מעילה (קנוניה זה שני עובדים ומעלה)
5. מהי הסיבה העיקרית לכפיית חופשה בארגון? 🡨 מניעת מעילה
6. השאלות הבאות מהמבחן!!!
7. מה מהבאים אינו נחשב הפרה של סודיות? 🡨 הרס חומרה
8. אלו מהבאים הוא עיקרון CIA המתכוון שלמישהו עם הרשאות יש גישה לאובייקט? 🡨 זמינות של המערכת
9. מנהל אבטחת המידע ביצע הערכת סיכונים בחברה. היה סיכון **שהיה בתאבון הסיכון** של החברה. הוא החליט להשקיע בבקרה מול סיכון זה 🡨 בזבז כספי החברה
10. פולס פוזיטיב הינה: 🡨 מאפשרת למישהו שאסור לו להיכנס
11. איזה מהמשפטים הבאים נכון לגבי קי לוגר? 🡨 יכולה לתעד אמצעי קלט שונים ללא ידיעת המשתמש
12. מהי אחת הסיבות העיקריות לכפיית חופשה על עובד? 🡨 כדי לאתר הונאה
13. מהי המטרה העיקרית של קרברוס? 🡨 אימות
14. הגנה בשכבות היא 🡨 מתודולוגיה להגנה על נכסי מידע קריטיים יותר מנכסי מידע לא קריטיים
15. סיכון שיורי הינו 🡨 הסיכון שנשאר לאחר הבקרות
16. העברת סיכון סייבר הינה 🡨 רכישת ביטוח
17. הפחתת סיכון הינה 🡨 יישום בקרות
18. מהו DMZ 🡨 demeliterized zone
19. פיירוול מתבסס על 🡨 חוקים
20. תקן ISO17002 הוא: 🡨 תקן בינלאומי לכללי אבטחת מידע
21. תקן PCI 🡨 לטיפול בכרטיסי אשראי
22. איזה עקרון מבטיח שהמשתמש לא יגיד שלא עשה משהו? 🡨 אחריותיות
23. מי מהבאים אינו דוגמה לסגמנטציה ברשת? 🡨 VPN
24. רשת מסוג בוטנט 🡨 משתמשת במחשבי זומבי ללא ידיעת בעליהם
25. התרחיש הבא הוא דוגמה למתקפה מסוג פישינג 🡨 מייל מזוייף
26. איזה מהבאים אינו יתרון של הצפנה אסימטרית? 🡨 מהירה
27. אקספלויט הינה תוכנה או קטע קוד 🡨 מנצלת פגיעות קיימת
28. מתקפות מסוג כופר או סחיטה 🡨 מצפינות את קבצי המשתמש בהצפנה אסימטרית
29. סייבר הוא 🡨 החיבור בין חומרה, תוכנה ואנשים למארג אחד
30. שלושת גורמי הסיכון העיקריים הם 🡨 טכנולוגיה, אנשים, תהליכים