

# הרצאה 1 - אבטחת מידע וסיבר - סיכום

## מסודר

---

מבוסס על מצגת ההרצאה (PPTX).

המסמך כולל את כל התוכן הכתוב המופיע בשקופיות, מסודר לפי סדר השקופיות.

## **ש��ופית 1: הרצאה 1**

## **ש��ופית 2: קורס: Information security and cyber**

מרצה: יניב מורדוב

## **ש��ופית 3: מרכיבי הציון בקורס:**

- מטלות ועבודות בית (לא העתקות): 10%
- השתתפות בכיתה: 10%
- מתכונת: 70%
- התרשומות מרצה: 10%

## **ש��ופית 4: מבוא לסייבר?**

סייבר הוא תחום רחב הכלול את כל היבטים הקשורים לאבטחת מחשבים, רשתות, תוכנות ומידע. המטרה העיקרית היא להגן על מידע ועל תשתיות מפני איוםים פוטנציאליים ולהבטיח שהמערכות יפעלו בצורה תקינה ובטוחה.

## שאיפית 5: היסטוריה של סייבר

תחום הסייבר החל להתפתח בשנות ה-70 עם הופעת המחשבים האישיים האישיים והרטות. עם השנים, ככל שה האינטרנט התפשט וה מידע נעשה חשוב יותר, התפתחו גם הטכנולוגיות והאינטראקטיבים הקשורים לסייבר. (נראה בהמשך דוגמאות לאינטראקטיבים שהתפתחו ממחמת העלייה בתוצר הטכנולוגיה)

## שאיפית 6: חשיבות הסייבר בעולם כיום

בעדן הדיגיטלי של היום, כל הארגונים והפרטים משתמשים על מערכות מחשב וניהול מידע. האינטראקטיבים בעולם הסייבר יכולים לגרום לנזק כלכלי עצום הבא לידי ביטוי בגניבת כסף מכיספומטים (נראה בהמשך הקורס איך עושים זאת), פגיעה בפרטיות ע"י פריצה וגניבת מידע אישי (כמו תמונות לא אטיות וכו'), ואףלו להשဖיע על ביטחון המדינה ע"י פריצה למערכות סופר מפוזרות שהחשיבות לשמירה בהם היא העליונה והגבוה ביותר.

## שאיפית 7: סוגי אינטראקטיבים סייבר:

- נזקות - נזקה פירושה תוכנה זדונית שתפקידה להזיק למחשב או לרשת המקומית (LAN) או הציבורית (WAN). זה כולל וירוסים, תולעים, וסוסים טרояניים. (נראה בהמשך כל אחד בפירוט מלא עם נפקא מינות להלכה)
- התקפות פישינג - התקפה שבה התוקף מתחזה לגורם אמין במטרה לגנוב מידע רגיש כמו סיסמאות לכל מיני מקומות וحسابות או פרטי אשראי. לדוגמה: דוא"ל מתחזה לבנק המבקש לאשר את פרטי החשבון. (נלמד בהמשך הלכה למעשה)
- התקפות מניעת שירות DDoS - התקפה שבה שולחים כמות עצומה של בקשות למערכת ספציפית ובכךanno גורמים לקריסתה ולהשבתת השירות.

- חדיות ווניבת מידע – תוקף שמצילח לחדר למערכות מחשב ולגנוב מידע רגיש מהמשתמש כמו פרטי לקוחות, מידע כספי ועוד.

## شكופית 8: דוגמאות מהעולם האמיתי:

- מתקפת וירוס ונאקיי - (WannaCry) נזקקה שהתרפשה למחשבים ברחבי העולם ע"י רשת האינטרנט וגרמה לנזק כלכלי גדול ע"י הצפת קבצים ובכך דרישת כופר.
- פרצת נתונים ב-Equifax - פרצת נתונים בחברת אשראי גדולה שבה נגנב מידע אישי של מעל ל- 140 מיליון לקוחות.

## شكופית 9: כלים וטכנולוגיות להגנה בסיבר

- חומות אש Firewalls – מכשירים (סנסורים) או תוכנות שמפקחים על התעבורה הנכנסת והויצאת מהרשות ומונעים גישה בלתי מורשית.
- אנט-ווירוס וכל מיני תוכנות הגנה – תוכנות שרצות על המחשב (אפשר שהיא באופן תמיד, אפשר עם ט"ימר מסוים, בדר"כ הם רצות בזמן הרצת המחשב ועם ט"ימר שמצויה היא המערכת של התוכנה) וברגע שהם מזוהות אז הם מסירות את נזקם מהמחשב.
- הצפנה Encryption - שיטה להבטחת (לשון להבטיח) סודיות המידע על ידי קידודו בצורה שלא מאפשר גישה ללא מפתח מתאים. [בהשمر הקורס נכנס לב העניין עם נפקא מינות הלכה למעשה]
- אימות דו-שלבי Two-Factor Authentication - תהליך שבו המשתמש צריך לספק שני אמצעים שונים לזיהוי (למשל סיסמה וקוד שנשלח לפלאפון הנייד).

## **שאיפית 10: המשך כלים וטכנולוגיות להגנה בסיביר**

כלים לניטור ותחקור- מערכות (SIEM) Security Information and Event Management המשמשות למציאת אירועים, גילוי חריגות, ותחקור התקפות.

## **שאיפית 11: עקרונות אבטחת מידע (CIA) - בסיס לאבטחת מידע**

- סודיות Confidentiality - שמירה על פרטי המידע כך שרק אנשים מורשים יוכל לגשת אליו ולעשות בו שימוש, כמו לדוגמה שנוכל להצפין קבצים ע"י SSL.
- שלמות Integrity - הבטחה שהמידע לא ישתנה ובנוסף גם לא יפגע ע"י גורמים שאינם מורשים, זהה ע"י חתימה דיגיטלית.
- זמינות Availability - הבטחה שהמידע ושירותי המערכת יהיו זמינים למשתמשים המורשים בזמן שהם זקוקים להם.

## **שאיפית 12: סודיות וחשיפה Confidentiality & Disclosure**

- שאלת: מה היא סודיות?
- תשובה: סודיות היא העיקרון הראשון של שמירה על פרטי המידע כך שרק אנשים בעלי הרשות יכולים לגשת אליו, כלומר אלו רוצים להבטיח מידע מסווג לאנשים שאינם צריכים להיחשף.
- דוגמאות:
  - הצפנת קבצים: נניח שאתה רוצה לשלוח מיל עם קובץ שמכיל מידע מסווג (כרטיס אשראי), ב כדי להגן על המידע, אתה מצפין את הקובץ, מה שעשו ההצפנה היא בעצם מוקדמת את המידע כך שרק מי שיש לו את המפתח המתאים יוכל לפענה ולקראת את הקובץ.

- שימוש בסיסמאות חזקות: באתר בנק הפעלים, אתה נכנס לחשבון שלך עם שם משתמש וסיסמה. הסיסמה היא שכבת הגנה שمبرטיחה לך את יכולך לגשת למידע החשבון שלך.
- אימות דו-שלבי: כדי להוסיף עוד שכבת אבטחה, ישנים אתרים הדורשים גם אימות נוספת כמו קוד שנשלח טלפון שלך, או קוד שנשלח מייל שלך, וכל זה בנוסף לסיסמה. וכך, גם אם מישהו יגלה את הסיסמה שלך, הוא עדין יצטרך את הקוד כדי להיכנס לחשבון.

## שוקפית 13: שלמות Integrity

- שאלה: מה היא שלמות?
- תשובה: שלמות היא העיקרי של שמירה על כך שהמידע לא ישתנה או יפגע על ידי גורמים שאינם מורשים. היינו רוצים להבטיח שהמידע "ישאר נכון ומדויק ולא יעשה בו שינויים שאין לנו רצם".
- דוגמאות:
- חתימה דיגיטלית: נניח שאתה מקבל חוזה במיל, החתימה הדיגיטלית שיש על החוזה מבטיחה לך שהחוזה לא שונה מאז שנחתם. כל שינוי במסמך יבטל את החתימה הדיגיטלית ויתגלה מיד.
- בדיקות שהנתונים שלמים ולא שונים: בארגון גדול כמו קריית נוער בסיס הנתונים שלו הוא גדול, יש מערכות שבודקות את הנתונים בכך לראות שהם לא נפגעו או שונים. לדוגמה, אם רשומות הליקוחות משתנות, המערכת תשליך התראה.

## שוקפית 14: זמינות Availability

- שאלה: מה היא זמינות?

- תשובה: זמינותו היא העיקרון של הבטחת הגישה למידע ולשירותים בזמן ובמקום הרצוי, קלומר אלו רוצים לוודא שהמערכות והמידע יהיו זמינים למשתמשים המורשים בכל עת וזמן שירצוז.
- דוגמאות:
- מערכות גיבוי ואחסון נתונים: חברות רבות משתמשות במערכות גיבוי כדי להבטיח שם יש תקלה במערכת הראשית, המידע עדין יהיה זמין. לדוגמה, אם יש בעיה במערכת השירותים, מערכת גיבוי תהיה אחראית לכך שהמידע לא יאבז ויהיה זמין לעובדים.
- התקפות מניעת שירות DDoS: כשמתתקפה מסווג SDoS מנסה להפיל אתר או שירות מסוון על ידי שליחת בקשות רבות, מערכות הגנה מיוחדות מופעלות כדי לסנן את הבקשות ובן להבטיח שהשירות ישאר זמין למשתמשים.

## שאלה 15: שאלה על עיקרון CIA

- בארגון גדול, ישנה מחלקה בשם צוותcia המישמת מדיניות אבטחת מידע מחמירה וכל זה ב כדי להגן על הנתונים הרגישים של החברה. הסבר כיצד כל אחד מהעקרונות הבאים - סודיות, שלמות וזמינות באים לידי ביטוי במדיניות אבטחת המידע של הארגון:
- סודיות: כיצד הארגון מבטיח שרק אנשים מורשים יכולים לגשת למידע רגיש?
- שלמות: איזה אמצעים נעשים בכך להבטיח שהמידע נשאר נכון ומדויק ולא משתנה ללא הרשותה?
- זמינות: אילו צעדים ננקטים כדי להבטיח שהמידע והשירותים יהיו זמינים למשתמשים המורשים בכל זמן שירצוז?

## **CIA - תשובה (א)**

- סודיות - הארגון מיישם מערכת בקירה שמאוד מkapidea ובנוספ' מבטיחה שרק עובדים מורשים יכולים לגשת למידע רגיש. כל משתמש חייב להיכנס עם שם משתמש וסיסמה "יחודיים", ולעתים קרובות גם עם אימות דו-שלבי.
- בנוסף, המידע הרגיש מוצפן תמיד (במנוחה וגם בתנועה), כך שגם אם הפורץ מצילח להשיג גישה למערכת, הוא לא יוכל לקרוא את המידע ללא המפתח המתאים.

## **CIA - תשובה (ב)**

- שלמות - הארגון משתמש בחתימות דיגיטליות כדי להבטיח שהמסמכים והנתונים לא שוננו לאחר יצירתם או חתימתם. כל שינוי במסמך מבטל את החתימה הדיגיטלית ומצביע על כך שהמידע שונה.
- בנוסף מערכת לניהול גרסאות וティיעוד שינויים מתבצעות בכל פעם שמסמך נערך, כך שניתן לעקב אחר כל השינויים ולהחזיר לגירסה הקודמת במקרה של שינויים בלתי מורשים.

## **CIA - תשובה (ג)**

- זמינות - הארגון מיישם מערכותגיבוי ו恢חזר נתונים כדי להבטיח שהמידע זמין גם במקרה של כשל המערכת הראשית. הגיבויים מתבצעים תמיד ונשמרים במקרה בטוח.
- בנוסף הארגון משתמש בעוד סוג רשותות וגם במערכת המפחיתה את העומס זהה בכך לוודא שהשירותים ישארו זמינים גם במקרה של עלייה חדה בעומס או תקלת מסוימת במערכת.

## שאיפית 19: גורמים שיוצרים סיכון לאבטחת מידע

הקדמה: גורמים שיוצרים לי סיכון באבטחת מידע הם הגורמים שיכולים להשפיע על הסיכון הכללי לארגון בגין אבטחת המידע שלו. חשוב מאוד להבין ולהעריך גורמים אלו לצורך זיהוי איוםים, הערכת סיכוןם, ותכנון השלבים הבאים המתאימים לניהול ולצמצום הסיכוןם. להלן בשאיפיות הבאות נראה מספר גורמי מרכיבי סיכון מרכזיים.

## שאיפית 20: אי ו-ם Threats

- איוםים הם פעולות שלוליות לגורם נזק למידע או למערכת המידע שלנו.
- דוגמאות:
- התקפות סייבר, כמו פישינג, מתקפות מניעת שירות DDoS ותוכנות זדוניות.
- גורמים פנימיים, כמו עובדים לא מרצים, טעויות אנוש.
- גורמים טבעיים, כמו שריפות, שיטפון, רעידות אדמה.

## שאיפית 21: פגיעות Vulnerabilities

- פגיעות הם חולשה במערכת כך שיכולה להיות מנצלות על ידי איוםים כדי לגרום לבאלגן.
- דוגמאות:
- חולשות תוכנה, למשל באגים, פגיעות אבטחה.
- נהלים לקוים, כמו סיסמאות חלשיות, ניהול גישה לא נכון.
- תשתיות לא מאובטחות, כמו רשותות לא מוצפנות.

## שקיופית 22: חשיפה Exposure

- חשיפה מתארת את האפשרות שבה המידע או המערכת חשופים לאיומים ולפגיעות.
- דוגמאות:
  - גישה פיזית לא מאובטחת למערכות המחשב.
  - חיבורם לא מאובטחים לרשותות חיצונית.
  - שימוש בשירותי ענן ללא אמצעי אבטחה מתאימים.

## שקיופית 23: השלכות Impacts

- השלכות הן התוצאה השנייה יהיה אפשר לקבל לאחר שהה אירוע אבטחה מוצלח, כולל הנזק שנגרם.
- דוגמאות:
  - אובדן מידע, כמו אובדן מסמכים חשובים, נתוני לקוחות.
  - נזק פיננסי, כמו הפסדים כלכליים, קנסות.
  - פגיעה במוניטין, כמו אובדן אמון לקוחות.

## שקיופית 24: גורמי מרכיבי סיכון - בתהליכיים

- קודם כל נסביר מהם תהליכיים (תלמדו בהמשך עם ד"ר יחזקאל גיא): תהליכיים הם כלליים ונחלים שהארגון מגדר כדי לנוהל ולתחזק את מערכות המידע שלו. גורמי סיכון בתהליכיים נובעים מחולשות או כשלים בתהליכיים אלו.
- דוגמאות:

- נהלי עבודה לא מתאימים - אם הארגון לא מגדיר נהלים ברורים לאבטחת מידע, כמו מדיניות סיסמאות חזקות או ניהול גישה למידע רגיש, יתכן שייהיו חורים בתהליכי האבטחה.
- חוסר בבדיקות ותיעוד - אם לא מתעדים שינויים במערכות ולא מבצעים בקרות שוטפות, יכול להיות שלא ישימו לב לשינויים בלתי מורשים או בעיות שנוצרות.
- תהליכי גיבוי ו恢復 לא יעילים - תהליכי גיבוי ו恢復 לא נכון או לא מתוגבל יכול לגרום לאובדן מידע קריטי בזמן חירום.

## **שאיפית 25: גורמי מרכיבי סיון - בטכנולוגיות**

- טכנולוגיות הן הכלים שהארגון משתמש בהם וזה בישבול לנחל ולאבטח את מערכות המידע. גורמי סיון בטכנולוגיות נובעים מפיגיעותמערכות או שימוש לא נכון בטכנולוגיות.
- דוגמאות:
- חולשות תוכנה - מערכות הפעלה ותוכנות יכולות להכיל פגיעות שגורמות לחשיפת מידע או פריצה למערכת.
- תשתיות לא מאובטחות - רשתות תקשורת לא מאובטחות או חוסר הצפנה (סימטרי או אסימטרי) יכולים לאפשר האזנה או גניבת מידע.
- חוסר עדכונים ותיקונים - אם לא מעדכנים את התוכנות באופן תקין, הן נשארות פגיעות לפרצות אבטחה ידועות.

## **שאיפית 26: גורמי מרכיבי סיון - אנושיים**

- הגורם האנושי הוא אחד הגורמים החשובים ביותר בכל סוגיית אבטחת המידע. מרכיבי סיון אנושיים נגזרים מההתנהגות, ידע של האנשים בחברה.
- דוגמאות:

- טעויות אנוש - עובדים יכולים בטעות להזין מידע שגוי, לשוכח לעדכן סיסמות, או ללחוץ על קישורים זדוניים.
- חוסר מודעות - עובדים שלא מודעים לסיכונים באינטרנט עשויים ליפול למלכודות פישינג או להוריד תוכנות זדוניות (XSS).
- גורמים זדוניים פנימיים - עובדים לא מרצים או כאלו שיש להם גישה למידע רגשי יכולים לנצל את הגישה שלהם כדי לגרום נזק מתוך נקמה למקום, או ממוקם של איזומים.

## שאפית 27: שאלה על גורמי מרכיבי סיכון

- חברת קריית נוער החליטה לבצע הערכת סיכונים מקיפה למערכות המידע שלהם. במסגרת ההערכתה, זוהו מספר פגיעות, איזומים וחסיפותמערכות השונות. בהתבסס על המידע הבא, נתן את הסיכונים המוצגים והתאם לכל אחד מהם את גורמי הסיכון הרלוונטיים - תהליכי, טכנולוגיות ואנושיים.
- א. פגיעות - חוסר עדכון קבוע של מערכות הפעלה ותוכנות על שרתיים. נהיי גיבוי וzechor נתונים אינם מתורגלים באופן קבוע ואני מתועדים כמו שצරיך.
- ב. איזומים - התקפות פישינג שמכוונות לעובדי הארגון, שמטרתן לגנוב אישורי גישה למערכות פנימיות. תוכנות זדוניות שמופצות בראשת הפנים עקב הורדות בלתי מבוקרות של קבצים מהאינטרנט.
- ג. חסיפות - רשות אלחותית פנימית שאינה מוצפנת ואני מאובטחת כראוי. גישה פיזית בלתי מוגבלת לחדרי שרתיים ואזרחי עבודה מאוד מאוד רגשיים.
- לאחר שקבלת את המידע הנ"ל: עלייך סטודנט יקר לפרט את גורמי הסיכון המיוחסים לכל פגיעות, איזומים וחסיפות. הסבר כיצד ניתן לצמצם או לנחל כל אחד מהסיכונים המוזכרים.

## **שוקפית 28: תשובה - גורמי מרכיבי סיכון**

- על בעית - חוסר עדכון קבוע של מערכות הפעלה ותוכנות על השרתים.
- גורם סיכון - טכנולוגיות
- פתרון - יש להפעיל מצב של עדכוני אוטומטיים למערכות הפעלה והתוכנות על השרתים.  
בנוסף יש לעקוב אחרי ההודעות על עדכוני אבטחה מיצרי התוכנה ולהתקין אותם ללא אפשרות דחיה.
- על בעית - רשות אלחותית פנימית שאינה מוצפנת ואינה מאובטחת.
- גורם סיכון - טכנולוגיות
- פתרון - כדי להפעיל הצפנה חזקה על הרשות האלחותית, ובנוסף להשתמש בשיטות אימוץ חזקות.

## **שוקפית 29: תשובה - גורמי מרכיבי סיכון**

- על בעית - נהלי גיבוי ו恢復 נתונים אינם מתורגלים ואינם מתועדים כראוי.
- גורם סיכון - תהליכיים.
- פתרון - צריך ליצור נהלי גיבוי ו恢復 מסודרים ולבדוק שהם מתועדים ומתורגלים באופן סדייר. זה כולל ביצוע בדיקות תקופתיות לוודא שהגיבויים מתבצעים בצורה נכונה ושה恢復 נתונים מתבצע כמו שצריך.

## **שוקפית 30: תשובה - גורמי מרכיבי סיכון**

- על בעית - התקפות של פישינג שמכוונות לעובדי החברה.
- גורם סיכון - אנושיים

- פתרון - צריך לקיים דרכים לעובדים בנוגע להתמודדות עם התקפות של פישינג, בנוסף יש להפעיל מערכות לסינון מיילים כדי להוריד את הסיכון שהודעות פישינג יגיעו לתיבות למיילים של העובדים של העובדים.

# הרצאה 2 - אבטחת מידע וסיבר - סיכום

## מסודר

---

מבוסס על מצגת ההרצאה (PPTX).

המסמך כולל את כל התוכן הכתוב המופיע בשקופיות, מסודר לפי סדר השקופיות.

## שאיפית 1: הרצאה 2

מרצה: יניב מורדוב

## שאיפית 2: מודל הכוכב - STAR MODEL

- טוב, אז תלמידי היקרים מהו מודל הכוכב – לא, זה לא טופולוגיה כוכב של תקשורת (תשאלו את מרגי).
- מהו מודל הכוכב? מודל הכוכב הוא מודל ניהול סיכון אבטחת מידע בחברות שונות. המודל תפקידו להציג בצורה פשוטה ומובנית את המרכיבים השונים של אבטחת המידע בחברה שלנו, ולהראות כיצד הם קשורים זה לזה. המודל מבוסס על כך שבמרכז הכוכב נמצא הליבה שהוא בעצם המידע החשוב ביותר שמוגן על ידי מספר שכבות הגנה – כMOVEDן בהמשך תהיה דוגמא מעשית בכך שנוכל לשכך את האוזן.

## שאיפית 3: ממה מורכב מודל הכוכב?

- במודל הכוכב, יש חמישה מרכיבים מרכזיים המוצגים ע"י קוודקודים של כוכב, וכל אחד מהם מייצג תחום חשוב באבטחת מידע, ואלו הן:
  - 1. אנשים People
  - 2. תהליכי Processes
  - 3. טכנולוגיה Technology
  - 4. סביבה Environment
  - 5. ניהול סיכונים Risk Management
- ועכשו ב-5 מצגות הבאות אנו נפתח ונסביר כל אחד אחד מהם.

## **שיקופית 4: מרכיב מודל הכוכב - אנשים**

- מרכיב: אנשים People
- ביאור העניין: האנשים בארגון הם אחד המרכיבים החשובים ביותר באבטחת מידע. הם כוללים את כל העובדים, מנהליים, ספקים ושותפים (כל מיני סוגים של שותפים, והם בין).
- אפשרות שיכולה לסייע בדבר: הדרכה, מודעות, ניהול זהויות והרשאות.
- לדוגמה: קיום הדרכות באבטחת מידע וסיבר לעובדים יכול לעזור למנוע התקפות של פישינג.

## **שיקופית 5: מרכיב מודל הכוכב - תהליכי**

- מרכיב: תהליכי Processes
- ביאור העניין: תהליכי הנהלים והמדיניות של הנהלים את אופן העבודה של החברה בתחום אבטחת מידע.
- אפשרות שיכולה לסייע בדבר: מדיניות אבטחת מידע, ניהול גיבוי ו恢復, בקרת גישה.
- לדוגמה: תהליך מוגדר לשחזור מידע במקרה של תקלת כל שהיא במערכת של החברה.

## **שיקופית 6: מרכיב מודל הכוכב - טכנולוגיה**

- המרכיב: טכנולוגיה Technology
- ביאור העניין: הטכנולוגיות הן הכלים והמכשורים המשמשים לאבטחת מידע בארגון.
- אפשרות שיכולה לסייע בדבר: שימושמערכות הגנה כמו אנטי וירוס והצפנה.
- לדוגמה: התקנת תוכנות של אנטי וירוס על כל המחשבים בחברה וכל זה כדי למנוע חדירות של תוכנות זדוניות.

## **שאיפית 7: מרכיב מודל בכוכב - סביבה**

- מרכיב: סביבה Environment
- ביאור העניין: הסביבה הפיזית והטכנולוגית שבה החברה פועלת.
- אפשרויות שיכולות לסייע בדבר: הגנה פיזית על מתקנים- כמו ליתן מאבטחים, ניהול גישה פיזית.
- לדוגמה: התקנת מצלמות אבטחה ובקרת גישה בחדרי שירותים.

## **שאיפית 8: מרכיב מודל הכוכב - ניהול סיכון**

- מרכיב: ניהול סיכון Risk Management
- ביאור העניין: ניהול הסיכון הוא תהליך של זיהוי.
- אפשרויות שיכולות לסייע בדבר: הערכת סיכון, ניטור שוטף, תגובה לאירועים.
- לדוגמה: ביצוע הערכת סיכון שנתי כדי לזהות ולהתמודד עם איומים חדשים.

## **שאיפית 9: כיצד מודל הכוכב עובד?**

- המודל יצא מנקודת הנחה שהחברה צריכה להגן על הליבה שהיא עצם המידע הרגיש, ע"י הקפדה על חמישה המרכיבים האלה. לכל מרכיב יש תפקיד חשוב בהגנה על המידע, וכשהם פועלים יחד בצורה, הם יוצרים הגנה מקיפה ועמידה כמעט לכל דבר.
- ועכשו נראה דוגמא לדבר..

## **שאיפית 10: דוגמא הلقה למעשה ליישום מודל הכוכב**

- החברה רוצה להגן על המידע הרגישי שלה.
- מרכיב: אנשים - הדרכות תקופתיות לעובדים על נהלי אבטחת מידע, בנוסף ליישום מערכת לניהול זהויות והרשאות כדי לוודא שרק אנשים מורשים יכולים לגשת למידע הרגישי.
- מרכיב: תהליכיים - כתיבת מדיניות אבטחת מידע ברורה ומפורטת, בנוסף קביעת נהלים לשחזור מידע וגיבויים קבועים.
- מרכיב: טכנולוגיה - התקנת מערכות אנטי וירוס על כל המחשבים והשרתים של החברה, בנוסף שימוש בהכנה למידע רגיש (וגם לצזה שלא כל כך רגיש).
- מרכיב: סביבה - התקנת מצלמות אבטחה ובקרות גישה פיזיות בחדרי משרדים ועוד, בנוסף הבטחת גישה פיזית למתקנים רק לאנשים מורשים ידועים.
- מרכיב: ניהול סיכונים - ביצוע של: הערכות, סיכונים תקופתיות, וכל זה כדי לזהות איומים חדשים גם ישנים, בנוסף ליישום מערכת לחיפוש בכל זמן ועת של פעילות רשות אוironium חריגים.

## **שאיפית 11: שאלה מסכמת על מודל הכוכב:**

- שאלה: חברת גודלה בשם M.YANIV.COM רוצה להטמע את מודל הכוכב לניהול אבטחת המידע שלו. במסגרת הטמעת המודל, נדרשת לבצע הערכה של כל אחד מרכיבי המודל שם: אנשים, תהליכיים, טכנולוגיה, סביבה וניהול סיכונים, ולזהות אפשרות פגיעה אפשריות.
- על הסטודנט (הינו עליך): לפרט ולהביא דוגמא אחת לכל מרכיב של המודל, המתארת פגיעות אפשרית בארגון.
- עליך להסביר כיצד ניתן להתמודד עם כל פגיעות שזוהתה, תוך שימוש בנהלים או טכנולוגיות מתאימות.

## **ש��ופית 12: (א) תשובה - מודל הכוכב**

- מרכיב: אנשים People
- פגיעה אפשרית: חוסר מודעות של העובדים לפישינג.
- דרכי התמודדות: לקים הדרכות מודעות אבטחת מידע לעובדים על זהות והימנעות מהתקפות של פישינג.

## **ש��ופית 13: (ב) תשובה - מודל הכוכב**

- מרכיב: תהליכי Processes
- פגעה אפשרית: חוסר בתייעוד ובביקורת תהליכי גיבוי ושחזר.
- דרכי התמודדות: כתיבת נלים מסודרים לגיבוי ושחזר, כך שייהי תיעוד, ובדיקות תקופתיות בכך שהגיבויים יבוצעו כראוי ושניתן יהיה לשחזר נתונים.

## **ש��ופית 14: (ג) תשובה - מודל הכוכב**

- מרכיב: טכנולוגיה Technology
- פגעה אפשרית: חוסר בהתקנת עדכנים וחוסר תיקונים לתוכנות.
- דרכי התמודדות: לישם מדיניות עדכנים אוטומטיים כך שלכל המערכת והתוכנות בחברה יבוצע הדבר מאליו, ומעקב אחר עדכוני אבטחה מיצרני התוכנה.

## שאיפית 15: (ד) תשובה - מודל הכוכב

- מרכיב: סביבה Environment
- פגיעה אפשרית: גישה פיזית בלתי מוגבלת לחדרי שירותים ואזרוי העבודה רגיסרים.
- דרכי התמודדות: התקנת מערכות בקרת גישה פיזית, כולל כרטיסי גישה ומצולמות אבטחה, וקביעת נחיי גישה ברורים.

## שאיפית 16: (ה) תשובה - מודל הכוכב

- מרכיב ניהול סיכון Risk Management
- פגעה אפשרית: חוסר ביצוע הערכות סיכון תקופתיות.
- דרכי התמודדות: ביצוע הערכות סיכון שנתיות לזיהוי איום חדשים וישום מערכות לחיפוש תמידי לאירועים לא רגילים.

## שאיפית 17: מודל שבע השכבות של: Depth in Defense

- מודל שבע השכבות של Depth in Defense הוא מודל שנועד להגן על מערכות מידע ע"י שימוש ברבדים רבים של הגנה ובטחה. הרעיון המרכזי במודל הוא שבמוקם להסתמך על שכבת הגנה אחת בלבד, יוצרים מספר שכבות הגנה, כך שאם שכבה אחת נפרצת, השכבות האחרות ימשיכו להגן על המידע.
- למודל הנ"ל 7 שכבות, ואלו הן:
  - 1. בטחת פיזית
  - 2. בטחת רשות
  - 3. בטחת היקף

- 4. אבטחת נקודת קצה
- 5. אבטחת יישומים
- 6. אבטחת נתונים
- 7.נהלים ומודעות – מדיניות
- \* ב-7 המציגות הבאים נסביר מה תפקידה של כל שכבה ושכבה במודל.

## **שוקפית 18: שכבה 1 של Depth in Defense**

- שכבה : אבטחה פיזית - Physical Security
- ביאור העניין: אבטחה פיזית מתיחסת להגנה על החומרה והמכשירים עצם מפני גישה בלתי מורשית, גניבה או נזק פיזי.
- לדוגמה: שימוש במנועלים, כרטיסי גישה, מצלמות אבטחה ושומרים.

## **שוקפית 19: שכבה 2 של Depth in Defense**

- שכבה: אבטחת רשת - Network Security
- ביאור העניין: אבטחת רשת מתמקדת בהגנה על תעבורת הרשת ועל המידע המועבר ברשת מפני התקפות וחדירות.
- לדוגמה: פירוקלים, מערכות זיהוי ומונעת חדירות IDS/IPS הצפנת תעבורת באמצעות VPN

## **שוקפית 20: שכבה 3 של Depth in Defense**

- שכבה: אבטחת היקף - Perimeter Security

- ביאור העניין: להגן על הגבולות החיצוניים של הרשת כדי למנוע חדירה ראשונית של גורמים עוינים.
- לדוגמה: פירוקלים היקפיים, סינון דוא"ל, סינון אתרים, שער רשות.

## שכופית 21: שכבה 4 של Depth in Defense

- שכבה: אבטחת נקודות קצה - Endpoint Security
- ביאור העניין: להגן על המרכיבים המוחברים לרשת כמו מחשבים, סרברים, פאלפונים חכמים ועוד - מפני התקפות.
- לדוגמה: אנטי וירוס, אנטי תוכנה זדונית.

## שכופית 22: שכבה 5 של Depth in Defense

- שכבה: אבטחת יישומים - Application Security
- ביאור העניין: להגן על האפליקציות השונות מפני פירצאות אבטחה שעלולות להוביל לחשיפה של נתונים רגישים מאוד או גישה בלתי מורשית למערכת של.
- לדוגמה: בדיקות חדירות יישומים, שימוש ב-WAF Web Application Firewall, פיתוח מאובטח Secure Coding (נדבר רבות בהמשך)

## שכופית 23: שכבה 6 של Depth in Defense

- שכבה: אבטחת נתונים - Data Security

- ביאור העניין: להגן על הנזונים עצם, בין אם במנוחה או בתנועה היינו בשימוש - מפני גישה בלתי מורשתית, שינוי או הריסה הרמטית.
- לדוגמא: הצפתת נתונים, גיבויים.

## **שאיפית 24: שכבה 7 של Depth in Defense**

- שכבה: מדיניות, נוהלים ומודעות - Policies, Procedures, and Awareness
- ביאור העניין: להגדיר את המדיניות והנהלים הנחוצים לשמירה על המידע של, ובנוסף להגבר את המודעות של העובדים לנושאי אבטחת המידע בחברה.
- לדוגמא: כתיבת מדיניות אבטחת מידע, הדרכות לעובדים, ובקורת נתונים.

## **שאיפית 25: שאלה מסכמת על Depth in Defense**

שאלת: בחברת ELIRAN\_SHUDED\_ZKENUT.COM מיושמת גישת Depth in Defense להגנה על מערכות המידע שלהם. החברה סובלת מהתקפות חוזרות על הישומים השונים שלה, המנצלות על ידי האקרים, וכל זה בכדי לגנוב נתונים אישיים. באילו שכבות של Model in Defense על החברה להתמקד כדי לטפל בבעיה הזאת, ובאליה צעדים מעשיים צריכים לנקט בכל שכבה ושכבה?

## **שאיפית 26: תש' בה:**

- עליינו להתמקד ב-3 שכבות וهم: אבטחת יישומים, אבטחת נתונים, ומדיניות נוהלים ומודעות.

- 1. אבטחת יישומים: לבצע בדיקות חדיות ליישומים בכך לזרות ותוקן פרצות אבטחה, בנוסף יש להשתמש ב-WAF בכך להגן על היישומים מפני התקפות נפוצות כמו SQL Injection ו-XSS, וגם ניתן לפתח בצורה מאובטחת Secure Coding על ידי שימוש בשיטות עבודה מומלצות לכתיבת קוד בטוח ושימוש בכללים לבדיקת קוד בזמן הפיתוח.
- 2. אבטחת נתונים: הצפת נתונים רגילים הנ בזמן שמירתם והן בזמן שליחתם, ובנוסף לבצע גיבויים סדריים של הנתונים ולשמור אותם במקום בטוח. ואפשר גם שימוש בקרת גישה מבוססת תפקודים בכך להגביל את הגישה לנ נתונים רק לאנשים ספציפיים ולא לכלם.
- 3. מדיניות נHALIM ומודעות: כתיבת מדיניות אבטחה מייד שמנדרה את הדרישות להגנה על יישומים ונתונים וכן כדי לעשות הדרישות לעובדים בנושא אבטחת יישומים ונתונים בכך להעלות את המודעות לסייעים ולדעת כיצד מגנים, וצריך גם לבצע ביקורת סדירה על היישומים והנתונים בכך להבטיח עמידה במדיניות ובנהלים.

# הרצאה 3 - אבטחת מידע וסיבר - סיכום

## מסודר

---

מבוסס על מצגת ההרצאה (PPTX).

המסמך כולל את כל התוכן הכתוב המופיע בשקופיות, מסודר לפי סדר השקופיות.

## **ש��ופית 1: הרצאה 3**

מרצה: יניב מורדוב

## **ש��ופית 2: אבטחת תשתיות מחשב**

- אבטחת תשתיות מחשב עוסקת בהגנה על כל המרכיבים הפיזיים והוירטואליים של מערכות מחשב, לדוגמה: מחשבים, שרתים, רשתות ואמצעי אחסון. האבטחה כוללת אמצעים להגנה מפני איומים פנימיים וחיצוניים, תוך שמירה על זמינות סודיות ושלמות המידע (CIA).
- לאבטחת תשתיות מחשב ישנים מספר צדדים, כרגע אנו נתמקד בסוגית אבטחה על מחשב בודד!

## **ש��ופית 3: אבטחה על מחשב בודד**

- אבטחת מחשב בודד מחולקת להרבה תחומיים ואלו הם:
  - 1. התקנת מערכת הפעלה מאובטחת - התקן מערכת הפעלה מעודכנת ונתמכת כמו: Linux, Windows 10
  - 2. הגנה באמצעות סיסמה - קבע סיסמאות חזקות לכל החשבונות במחשב, וגם השתמש באימות דו שלבי כאשר אפשרי, ובנוסף אל תשמור סיסמאות בצורה גלויה במחשב שלך.
  - 3. תוכנות אבטחה - התקן אנטי וירוס ואנטי תוכנה זדונית, בצד להגן על המחשב מפני וירוסים ותוכנות זדוניות וטוב גם לבדוק WHETHER התוכנה מעודכנת ומtbodyות סריוקות כל פרק זמן מסויים.

- 4. פירול Firewall - הפעל את הפירול המובנה במערכת הפעלה כדי להגן על המחשב מפני גישה בלתי מורשית, ואם אתה כל כך רוצה או צריך התקן פירול נוסף להגדלת רמת ההגנה.
- 5. הצפנה נתונים - הצפן את הדיסק הקשיח באמצעות כלי הצפנה כמו BitLocker ב- macOS (מאוד מומלץ), וגם טוב להשתמש בהצפנה קבצים Windows FileVault עבור נתונים אישיים.

#### **שकופית 4: המשך דרכי אבטחה על מחשב בודד**

- 6. גיבויים – יש לבצע גיבויים סדריים של הנתונים החשובים במחשב, וגם לשמר גיבויים במקום בטוח ונפרד מהמחשב לדוגמא: כונן חיצוני או שירות ענן.
- 7. עדכוני תוכנה – לבדוק שכל התוכנות המותקנות במחשב מעודכנות לגרסה الأخيرة, ובנוסף יש להפעיל עדכונים אוטומטיים בכך לקבל את כל התיקונים והעדכונים הנדרשים בזמן.
- 8. מודעות והדרכה – למד את המשתמשים על ניהול אבטחה, כמו זיהוי פישינג, אי פתיחת קבצים מצורפים לא מזוהים, ולא להוריד תוכנות ממוקורות לא אמינים.
- 9. הרשותות וגישה – להציג הרשותות גישה מתאימות לכל המשתמשים במחשב, היינה להשתמש בחשבונות משתמש עם הרשותות מוגבלות לעבודה, והשתמש בחשבון מנהל רק כאשר יש צורך בכך.
- 10. ניטור ותגובה לאירועים – להתקין כלי לכך לעקב אחריו פעולות חשודות במחשב, וגם תתכן להגיב לאירועי אבטחה במהירות.

## ש��ופית 5: אבטחת חומרה

מה היא חומרה? חומרה הם כל הרכיבים הפיזיים במחשב, הינו מעבד, זיכרון, כונן הקשיח, לוח האם, ועוד. אבטחת חומרה מתמקדת בהגנה על רכיבים אלה מפני נזקים פיזיים, כמו: גנבה, שימוש ללא הסכמה.

## ש��ופית 6: כיצד לאבטח חומרה?

- 1. מנעולים פיזיים - שימוש בכבלים ומנעולים פיזיים בצד להבטיח שהמחשב לא יגנב. והוא הדין גם בעילית חדרי שרתים וחרדים המכילים מחשבים.
- 2. גדרות ומצלמות אבטחה - התקנת מצלמות אבטחה וגדרות בצד להגן על אזורים שדרושים שמירה והגנה, וגם מעקב אחר פעילות חשודה במקומות שבהם נמצא החומרה שלנו.
- 3. שמירה על הסביבה הפיזית - שמירה על סביבה מתאימה, זה בא לידי ביטוי בטמפרטורה, לחות וכל זה בצד למנוע נזקים לרכיבים שונים.
- \* טוב להתקין מערכות גיבוי شامل כמו UPS כדי למנוע נזקים כתוצאה מהפסקות شامل.

## ש��ופית 7: אבטחת קושחה

מה היא קושחה? קושחה Firmware היא התוכנה המובנית בתוך רכבי החומרה, כמו ה-BIOS או ה-UEFI בלוח האם, תוכנת הבקרה במעבדים, בקרני רשת, ועוד. אבטחת קושחה תפקידה בהגנה על תוכנה זו מפני התקפות שעלוות לשנות את פועלתה או לנצל פרצות אבטחה שבה הוכחה מחייבות.

## **ש��ופית 8: כיצד לאבטוח קושחה**

- 1. עדכוני קושחה - התקנת עדכוני קושחה מיצרן החומרה כדי לתקן פרצות אבטחה שהתגלו לאחר זמן, ובנוסף בדיקה תקופתית של עדכנים חדשים והתקנותם באופן תדרי.
- 2. הגנה על BIOS, UEFI - להגדיר סיסמה להגנה על ה-UEFI, BIOS בכך למנוע גישה לבلتி מורשים.
- 3. הצפנה ואיומות - לינטן לשימוש בטכנולוגיות הצפנה ואיומות בקושחה בכך למנוע שינוי בלתי מורשה או הזרקת קוד זדוני INJECTION גם לבדוק שהקושחה חותמה דיגיטלית בעת התקנתה.
- 4. גיבוי ו恢復 - גיבוי הקושחה חשובה כדי לאפשר恢復 במקרה של תקלת או שינוי של התוקף, כמוובן שמירה על גיבויים במיקום מאובטח ונפרד מהמחשב.
- 5. ניטור פעילות חריגה - להתקין כלי חיפוש לזיהוי פעילות חריגה בקושחה, כגון שינוי בלתי מורשה בהגדרות ה-UEFI, BIOS.

## **ש��ופית 9: \*(למעוניינים) במידה ואתם שמים סיסמה ב- BIOS:**

- שמור את הסיסמה במקום בטוח: אם תשכח את הסיסמה, יהיה קשה מאוד לשחזר אותה, ולפעמים נדרש ליצור קשר עם התמיכה הטכנית של היצרן.
- עדכן את הסיסמה באופן תקופתי: עדכן תקופתי של הסיסמה מגביר את רמת האבטחה.
- השתמש בסיסמה חזקה: השתמש בשילוב של אותיות, מספרים וסימנים מיוחדים.

## **שאפית 10: שאלת אבטחת חומרה וקושחה:**

- שאלה: חברת תוכנה בשם DANIEL.COM החליטה להקשייח את מערכם המחשב שלה בעקבות מתקפות סייבר חוזרות ונשנות. חלק מהטהלים, החברה רוצה להבטיח שף אחד לא יוכל לשנות את הגדרות BIOS או להעלות מערכת הפעלה לא מאומנת.
- 1. הסבר כיצד ניתן להגן על הגדרות-h-UEFI/BIOS מפני גישה בלתי מורשתית?
- 2. גם מדוע חשוב להפעיל אפשרות של Secure Boot ?

## **שאפית 11: תש בה:**

- 1. הגדרת סיסמה ל-UEFI/BIOS : כדי להגן על הגדרות-h-UEFI/BIOS יש להגדיר סיסמת ניהול מערכת Administrator Password ואנו צריכים סיסמה זו בכדי לגשת ולשנות את הגדרות-h-UEFI/BIOS. ובנוסף ניתן להגדיר סיסמת משתמש שתידרש בעת אתחול המחשב, כך שרק מי שמכיר את הסיסמה יוכל לאותחל את המחשב.
- 2. מודוא שרק תוכנות מערכת הפעלה מאומנות וחתוםות דיגיטליות על ידי הייצן יטענו במהלך אתחול המחשב ולא דברים אחרים. ובנוסף זה מונע מתוכנות זדוניות להיטען ולהציג שליטה על המחשב עוד לפני שמערכת ההפעלה נטענת וחושב גם לדעת שהפעלת Secure Boot מסייעת בהגנה על שלמות מערכת האתחול ומפחיתה את הסיכון לניצול פגיעות קרייטיות במערכת.

## **שאפית 12: הקשהת מערכת הפעלה**

- מהי הקשהת מערכת הפעלה?

- הקשהת מערכת הפעלה (OSH) היא תהליך של חיזוק ההגנות והקטנת הפגיעות של מערכת הפעלה מפני התקפות סიכוניים. תפוקידנו להפחית את מספר הנזקודות הפגיעות שבמערכת שיכולה להיות מנצלות על ידי תוקפים ובכך להבטיח שמערכת הפעלה תהיה כמו שיוטר מאובטחת ולא פגעה.

### **שאיפית 13: השלבים להקשהת מערכת הפעלה:**

- 1. עדכונים ותיקונים Patching: צריכים אנו לוודות שכל העדכנים והתיקונים האחרונים של מערכת הפעלה מותקנים אצלנו, ובנוסף הפעל עדכנים אוטומטיים כדי לקבל תיקונים חדשים באופן עצמוני.
- 2. הגדרות אבטחה Security Settings: עדכן את הגדרות האבטחה המובנות של מערכת הפעלה, וגם תזודא שהגדרות האבטחה המומלצות מושמות.
- 3. הגנה על חשבון משתמש: השתמש בסיסמאות חזקות לכל החשבונות, וטוב גם להשתמש באימות דו שלבי עבור חשבונות המשתמשים.
- 4. כיבוי שירותים ותוכנות לא נחוצים: נטרל שירותי ותוכנות שלא בשימוש בכדי לצמצם את שטח התקיפה.
- 5. פירwall Firewall: הפעיל את הפירwall המובנה במערכת הפעלה, ובנוסף הגדר כלליים מגבלים לגישה מרשות חיצונית.
- 6. אנטי-וירוס ואנטי תוכנה זדונית: התקן תוכנות אנטי-וירוס ואנטי-תוכנה זדונית, ובנוסף תזודא שהתוכנות מעודכנות ומתבצעות סריקות بصورة תדירה.

## שאיפית 14: המשך - שלבים להקשות מערכת הפעלה

- 7. הצפנה: הצפן את הוכן הקשיח באמצעות BitLocker ב-Windows (וכל מערכת ההפעלה ההצפנה תהיה ע"י תוכנה אחרת), ובנוסף השתמש בהצפנה קבצים עבור נתונים רגישים.
- 8. ניהול עדיפויות Permissions Management - הגבל את הגישה לקבצים ותיקיות רגישות, ובנוסף הגדר הרשות גישה מתאימות למשתמשים ולתוכנות ספציפיות.
- 9. הגנה על רשות: השתמש ב-VPN לגישה מרוחיק, ובנוסף תודא שמכשרים מחוברים לרשת מאובטחת.
- 10. ניטור ובקרה: התקן כל ניטור לדיזהו פעילות חריגה, ובנוסף הקם מערכת התראות להתראה מיידית על אירועי אבטחה.
- 11. בקרת גישה: השתמש ב-(ACLs) Access Control Lists לניהול גישה לקבצים ותיקיות.

## שאיפית 15: שאלת הבדיקה של מערכת הפעלה:

מסויימת מנסה באופן חוזר לגשת למערכת שלר ומציגת הtentations חדשה. כדי IP שאלת: כתובות זו באמצעות פירול. IP להקשיח את מערכת הפעלה שלר, עליך לחסום את הגישה מכתובת כדי לחסום iptables-המשתמש ב] עבור מערכת הפעלה לינוקס Bash - כתוב סקריפט פשוט ב [IP 192.168.1.100]

```
IP_TO_BLOCK="192.168.1.100"
```

```
sudo iptables -A INPUT -s $IP_TO_BLOCK -j DROP
```

# שמירת החוקים כר שישרו את חילוף מחדש של המערכת •

```
sudo sh -c "iptables-save > /etc/iptables/rules.v4"
```

- אנחנו רוצים לחסום את הכתובת הנ"ל, והוא נציב אותה במשתנה, ומיד אח"כ אנו משתמשים בפקודה בצד י' לחסום את הכתובת הנ"ל וכמוון גם כל תנועה מאותה הכתובת אנו חסמים, אנו ניגע בפקודות הללו שנגיע לפירול
- אנחנו משתמשים בפקודת את התנועה מכתובת ה-IP.

## שאפית 16: שאלה עיונית - דומה לשאלות בחינה סופית

- שאלה: מהי הטכניקה של "Least Privilege" וכייזד היא תורמת להקשות מערכת הפעלה?
- תשובה: טכניקת Least Privilege שזה בעצם הרשאות המינימליות, היא כוללת הגבלת הרשאות של משתמשים ותוכנות למינימום הרשאות הנחוצות לביצוע תפקידם. הדבר הזה תורם להקשות מערכת הפעלה על ידי צמצום הסיכוי לניצול הרשות יתר במקרה של פריצה או תקלה, וכך מגביר את האבטחה ומפחית את הנזק הפוטנציאלי מתוכנות זדוניות או משתמשים בלתי מורשים.

## שאפית 17: שאלה נוספת:

- שאלה: יוסי עובד כאיש סיסטם בחברת פיתוח תוכנה גדולה. לאחרונה, הוא קיבל דיווחים על כך שמערכות החברה סובלות מהתקפות חוזרות ונשנות של תוכנות זדוניות. בהערכת מצב הבטיחות של המערכת, הוא שם לב שחלק מהמחשבים מריםים ישומים שונים בהרשות ניהול, בעקבות כך יוסי החליט לבצע הקשות מערכת הפעלה כדי להגן על המחשבים והשרתים של החברה.

- כחלק מהפעולות להקשות מערכת הפעלה, יוסי החליט להפעיל את מגנון ה-UAC (בקשה על המשתמשים) במחשביו החברה. הסבר מהו מגנון ה-UAC וכייזד הוא תורם להקשות מערכת הפעלה ולהגנה מפני תוכנות זדוניות.

## שאיפית 18: תש בה:

- מגנון ה-(User Account Control) UAC הוא תכונה אבטחה במערכות הפעלה Windows שמטרתה להגביל את הרשאות של תוכנות ומשתמשים, על מנת להפחית את הסיכון לנזקים ממוקור תוכנות זדוניות ושגיאות משתמש.
- ה-UAC תורם להקשות מערכת הפעלה ולהגנה מפני תוכנות זדוניות על ידי:
  - בקרת הרשאות: UAC מודרש אישור מהמשתמש לפני הרצת "ישומים" חדשניים הרשות מנהל, מה שמקשה על תוכנות זדוניות לבצע פעולות מזיקות ללא ידיעת המשתמש.
  - הרצת "ישומים" בהרשאות מוגבלות: כבירית מחדל, "ישומים" רצים בהרשאות משתמש רגיל, וההרשאות מוגבלות מורידות את הסיכון לניצול פרצחות בתוכנה.
  - מניעת התקנות לא מורשות: UAC מקשה על התקנת תוכנות חדשות ללא אישור מפורש של המשתמש עם הרשות מתאימות.

## שאיפית 19: הקשת רכבי תקשורת

- חברת WANIC.COM היא חברת טכנולוגיה עם משרדים רבים ברחבי העולם. يوم אחד, צוות האבטחה גילה שיש תנוצה בלתי רגילה בראש החברה. חקירה מהירה העלתה ששרותים רבים במשרדים המרכזיים החלו לשלוח נתונים גדולים לכתובת IP זרה.

- צוות האבטחה הבון במהירות שמדובר בפריצה רצינית, והחל בניתוח האירוע. הסתבר שתוכפים הצלחו לפרט מרכזיו שהיה מוגדר עם סיסמת ברירת מחדל. לאחר הפריצה, התוקפים יכולים להקל על התעבורה ברשות ושלוט בה.
- ובגלל הבעייה בנתב, שהנתב הינו רכיב תקשורת אנו צריכים להקשיט.

## **שאיפית 20: כיצד מKeySpecים רכבי תקשורת:**

- 1. שינוי סיסמאות ברירת מחדל: במקרים רבים, תוכפים מצליחים לחדר לרשות פשוט על ידי שימוש בסיסמאות ברירת מחדל של רכבי הרשות. לדוגמה, תוכף שהצליח להיכנס למציג רשות במפעל גדול, הצלח להשתלט על כל תעבורת הרשות פשוט על ידי כניסה עם סיסמה ברירת המחדל.
- از מה עושים? יש לשנות את סיסמאות ברירת המחדל של כל רכבי התקשרות לסיסמאות חזקות וייחודיות מיד עם התקנתם.
- 2. עדכוני תוכנה וקושחה Firmware: בשנת 2018, פרצה נחשפה בקושחת נתב פופולרי, שמאפשרת לתוכפים להשתלט על הנתב מרוחק. התקפות רבות ניצלו את הפרצה עד שיצר הנتاب פרסם עדכון קושחה שתיקן את הבעייה.
- از מה עושים? יש לעדכן את הקושחה והתוכנה של רכבי התקשרות באופן קבוע. עדכנים אליהם כוללים לעיתים קרובות תיקוני אבטחה לחולשות שהתגלו.
- 3. ניהול גישה והרשאות: חברת ייעוץ גלובלית גילתה שתוקף הצלח להשתלט על חשבונן ניהול מערכות של מציגי הרשות התוקף השיג גישה דרך חישובן עם הרשאות גבוהות שלא היה נדרש להיות פעיל.
- از מה עושים? יש להגדיר הרשאות מינימליות Least Privilege לכל משתמש ויישום, ולודא שרק מי שצריך גישה יוכל אותה.

## שאיפית 21: המשך הקשחת רכיבי תקשורת:

- 4. הגבלת גישה מרוחק: במתකפה על בנק מקומי, התוקפים השתמשו ב프וטוקול Telnet כדי לגשת לנטים ולשנות את הגדרותיהם, מה שאפשר להם לירט תעבורת ולגנוב נתונים רגילים.
- מה עליינו לעשות? יש להגביל את הגישה מרוחק לרכיבי הרשות ולהשתמש בשיטות גישה מאובטחות כמו VPN ו- SSH במקומם פרוטוקולים פחות מאובטחים כמו Telnet.
- 5. שימוש בפרוטוקולי תקשורת מאובטחים: ארגון רפואי גילה שהתקפות -in (Man-in-the-Middle) מתבצעות על התקשרות שלהם, משומם שהם השתמשו בפרוטוקול HTTP לא מוצפן לשילוח נתונים בין שרתים.
- מה עליינו לעשות? יש להשתמש בפרוטוקולים מאובטחים כמו HTTPS במקום HTTP, ו- SNMPv3 במקום גרסאות ישנות יותר של SNMP.
- 6. יישום בקרות גישה מבוססות כתובות (ACLs) IP: חברת לוגיסטיקה הצליחה למנוע מתකפת סייבר כשהשתמשו ב-ACLs כדי לחסום תעבורת חשודה מכותבות IP זרות שזויה בניסיונות גישה לא מורשים.
- וכן יש להגדיר ACL כך שיגבילו את הגישה לרכיבי הרשות על פי כתובות IP מאושזרת בלבד.
- 7. ניטור והתרעה: בית חולים גילה מתකפה על מערכותיו רק לאחר שהמערכות התריעו על תעבורת חריגה לשירותים חיצוניים בשעות הלילה. בזכות מערכות הניטור, הצלicho להפסיק את ההתקפה בזמן.
- וכן טוב מאוד להטמע מערכות לניטור והתרעה SIEM שיתריעו על פעילות חריגה ואי אפשרו לתגובה מהירה לאירועים חשודים.
- 8. פיצול רשות: חברת ייצור הצליחה לצמצם את הנזק מהתקפת כופרה (virus) Ransomware על ידי פיצול הרשות שלה כך שהתקפה לא יכולה להתרפשט למקטעים קרייטיים אחרים של הרשות.

- ולכן יש לפצל את הרשות למקטעים שונים כך שהגישה בין המקטעים תהיה מוגבלת ותתבצע דרך נקודות פיקוח מאובטחות. זה מנסה על תוקף נוער ברחבי הרשות אם הצליח לפרוץ לאחד המקטעים.

## שאלה 22: שאלת

- בחברת ELIRAN\_AND\_DANIEL עבד צוות[T] שהשיקיע רבות באבטחת הרשות. يوم אחד, המנכ"ל קיבל דוא"ל אונומי שטען כי מערכת הרשות של החברה פגעה וחסופה לתקיפות. הדוא"ל הכיל פרטים על מספר רכיבי תקשורת שהיו בשימוש החברה עם סיסמאות ברירת מחדל.
- יניב הוא מנהל אבטחת המידע והוא גילה שמתגיה הרשות במשרדים הראשיים עדין השתמשו בסיסמאות ברירת מחדל שהיו ידועות לכל. יניב הבין שעליו להקים את רכיבי התקשרות בצורה מיידית!!
- tan 5 הצעדים העיקריים שיניב יוכל לנתקות להקשות רכיבי התקשרות של החברה, וכי צד שניי סיסמאות ברירת מחדל יכול למנוע התקפות בעtid?

## שאלה 23: תש'ה

- על יניב לעשות את הצעדים הבאים:
- 1. שינוי סיסמאות ברירת מחדל: אחד הצעדים הראשונים והחשובים ביותר הוא לשנות את סיסמאות ברירת המחדל של כל רכיבי התקשרות לסיסמאות חזקות וייחודיות. פעולה זו תמנע מתקופים להשתמש בסיסמאות ידועות כדי לגשת לרכיבים.
- 2. עדכוני תוכנה וקושחה: יש לוודא שכל רכיבי התקשרות מעודכנים לגרסאות התוכנה והקושחה האחרונות, אשר כוללות תיקוני אבטחה לחולשות שהתגלו.

- 3. ניהול גישה והרשות: הגדרת הרשות מינימלית למשתמשים ורכיבים כך שכל משתמש יקבל גישה רק למשאים הנחוצים לו.
- 4. הגבלת גישה מרוחק: שימוש בשיטות גישה מאובטחות כמו VPN ו- SSH במקום פרוטוקולים פחות מאובטחים כמו Telnet והגבלת הגישה מרוחק רק למשתמשים מורשים.
- 5. שימוש בפרוטוקולי תקשורת מאובטחים: יש להפעיל פרוטוקולים מאובטחים כמו HTTPS ו- SNMPv3 על רכיבי התקשרות.
- 6. ועוד ..
- \* וחשוב להזכיר שינוי סיסמאות ברירת מחדל לרכיבי התקשרות הוא קריטי משומם שsismאות ברירת מחדל ידועות לציבור ויכולות לשמש תוקפים לגישה לא מורשית לרשות. על ידי שינוי הסיסמאות, ניתן מצמצם את הסיכון להתרחשויות התקפות נוספות.

## **שאיפית 24: כלי חשוב שראינו לעיל**

כדי להגן על הרשות ניתן להשתמש בפקודה הזאת במקרה ברכי לחסום את כל התנועה - iptables. זו IP-הנכתנת מכתובה ה

sudo iptables -A INPUT -s 192.168.1.100 -j DROP

- אנו בעצם בשורת קוד הזאת בלינוקס נוכל לעצור את כל התעבורה מהכתובת IP הבאה: 192.168.1.100

## שאיפית 25: הבדיקה מסדי נתונים

- מסדי נתונים הם חלק חיוני מכל מערכת מידע, ומשמשים לאחסון וניהול כמויות גדולות של נתונים. אבטחת מסדי נתונים היא קריטית להגנה על המידע הרגיש של הארגון מפני איומים פנימיים וחיצוניים.
- חברת MARYAT.nOAR.jERUSALEM היא ספקית שירותי המחזיקה מסדי נתונים עם מידע רגיש של לקוחות. באחד הימים, תוקף הצלח לחדר למערכת החברה באמצעות מתקפת SQL Injection (שאותה נלמד לבצע בהמשך הקורס) בה הוא הזריק פקודות זדוניות לטופס חיפוש באתר החברה. דרך קר, התוקף השיג גישה בלתי מורשית למידע של אלפי לקוחות. וכך מחתם הבעה הזאת אנו ציריכם להוכיח את מסדי הנתונים שלנו.

## שאיפית 26: מה עליינו לעשות בבדיקה מסדי הנתונים:

- 1. אימות וניהול משתמשים: בחברת COM.VANITY חשבו מנהל מסד נתונים היה מוגדר ללא סיסמה חזקה, ותוקף הצלח לנחש את הסיסמה ולגשש למידע הרגיש.  
הבדיקה: שימוש בסיסמאות חזקות ומורכבות לכל המשתמשים, וגם הטמעת אימות דו-שלבי לגישה למסד הנתונים, ובנוסף הקצאת הרשות מינימלית על פי תפקיד המשתמש.
- 2. חברת אינטלק איבדה מחשב נייד שככל גבוי של מסד נתונים עם מידע רפואי רגיש שלא היה מוצפן. המידע גנוב והדליף לציבור.  
הבדיקה: הצפנת נתונים במנוחה ובתנועה וכל זה בכדי להגן על מידע רפואי, ובנוסף שימוש בתעודות SSL/TLS להבטחת תקשורת מוצפנת בין השירותים והלקוחות.
- 3. הגנה מפני SQL Injection: חברת CISCO נפגעה ממתקפת SQL Injection שחשפה את פרטי הלקוחות שלו. המתקפה הتبיעה על ידי הזרקת פקודות SQL זדוניות לטפסי הזמנות מקוונים.

- הקשחה: שימוש בפרמטרים או בייקטים מאובטחים של SQL למניעת הזרקות, ובנוסף הטמעת ספריות (Object-Relational Mapping) כמו Entity ORM או Hibernate (נדבר בהמשך הקורס)

## שאיפית 27: המשך - מה علينا לעשות בהקשות מסדי הנתונים:

- 4. ניהול עדכנים וטלאי אבטחה: בחברת COM.ELIRAN מסד הנתונים לא עודכן לגרסה الأخيرة, ונמצאה בו חולשת אבטחה קריטית. תוקפים ניצלו את החולשה לגנוב מידע של סטודנטים.
- הקשחה: עדכן שוטף של גרסאות מסד הנתונים והטמעת טלאי אבטחה ובנוסף שימוש בתהילכי CI/CD לבדיקת אבטחה וישום עדכנים באופן מתמיד.
- 5. גיבוי ו恢復 נתונים: חברת IL.CO.ULIEL חוותה מתקפת שבה השבתו מסדי הנתונים שלא. בגלל שלא היו גיבויים עדכנים, החברה איבדה נתונים קריטיים והייתה צריכה לשלם כופר גובה.
- הקשחה: גיבוי נתונים באופן קבוע ושמירת גיבויים במקום מאובטח. בדיקה תקופתית של תהליך השחזור כדי לוודא שניתן לשחזור את הנתונים במהירות במקרה של איבוד נתונים.
- 6. ניטור והתרעה: חברת AC.NOAN הצליחה למנוע גיבת מידע לאחר שמערכות הניטור שלא זיהו פעילות חשודה במסד הנתונים. התוקף ניסה לשאוב כמות גדולה של נתונים לצורכי לא רגילה.
- הקשחה: הטמעת מערכות ניטור והתרעה SIEM לניטור תעבורת מסד הנתונים וזיהוי פעילות חריגה, ובנוסף צריך לעשות ניתוח לוגי בכדי לזהות ולהגיב במהירות לאירועי אבטחה.

## שאיפית 28: שאלות על הקשחת מסדי נתונים:

- 1. מה ה יתרונות של שימוש באימות דו שלבי במסדי נתונים?
- 2. מהי מתקפת SQL Injection וכייז ניתן למנוע אותה?
- 3. מדוע חשוב לעדכן גרסאות מסדי נתונים באופן קבוע ולהטמיע טלאי אבטחה?
- 4. מהן הפעולות שיש לבצע כדי לוודא שניתן לשחזר את הנתונים מגיבויים במקרה של אובדן נתונים?
- 5. כיצד מערכות ניטור והתרעה יכולות לסייע בזיהוי ומונעת מתקפות על מסדי נתונים?

## שאיפית 29: תשובות על הקשחת מדוי נתונים:

- 1. אימות דו שלבי מוסיף שכבת אבטחה נוספת מעבר לסיסמה. כדי לגשת למערכת, יש צורך גם בפריט נוסף הדבר מקשה על התוקפים, ואפילו אם הם מושגים את הסיסמה בגלם שהם עדין זמינים לאותו פריט נוסף.
- 2. מתקפת SQL Injection מתרכשת כאשר תוקף מהציג פקודות SQL זהניות לתוך שאלתה של מסד הנתונים דרך קלט משתמש לא מסונן. וכך ניתן למנוע מתקפות כאלה על ידי שימוש בפרמטרים בשאלות Prepared Statements או על ידי הטמעת ספריות ORM (Object-Relational Mapping) שמטפלות באבטחת השאלות באופן אוטומטי.
- 3. עדכנים וטלאי אבטחה כוללים תיקונים לחולשות שהתגלו בגרסאות קודמות. השارة מערכת לא מעודכנת חושפת את המערכת לסיכון והתקפות שעוללות לנצל את החולשות הללו. לכן, חשוב לעדכן את המערכת ולשמור על אבטחתה.
- 4. יש לגבות נתונים באופן קבוע ולשמור את הגיבויים במיקום מאובטח, לבדוק באופן תקופתי את תהליכי השחזור כדי לוודא שהוא פועל כראוי, ולהיות מוכנים עם תוכנית שחזור שmaps את הצעדים לשחזר הנתונים במקרה של איבוד.

5. מערכות SIEM (Security Information and Event Management) מונטרות את התעבורה והפעולות במסד הנתונים, מנתחות לוגי וגם מזהות פעילות חריגה או חסודה בנסוףם יכולות לשלוח התרעות בזמן אמת ולהפעיל תהליכי אוטומטיים לטיפול באירועי בטחה, ובכך לסייע במניעת מתקפות או זיהוי מוקדם שליהן.

### שאיפית 30: דוגמא של קוד המונע SQL Injection

```
query = 'INSERT INTO users (username, password) VALUES (?, ?)'  
cursor.execute(query, (username, password))
```

- השתמשנו בפרמטרים בצד ימין של SQL Query וע"י הפקודה הנ"ל מקבלת השאלה את הפרמטרים כתאפלים, מה שמנע הזרקת SQL.
- הבהיר לנו נלמד בעין איך וכייך מזրיכים - אל תdagו הכל יהיה בסדר

### שאיפית 31: אבטחת מכשירים ניידים

- פתחה לחכמה: מכשירים ניידים כמו טלפונים חכמים וטאבלטים הם חלק בלתי נפרד מחינינו. אנו משתמשים בהם לאחסן מידע אישי ועסקתי רגשי, מה שמעמיד אותנו כיעד מרכזי למתתקפות סייבר. אבטחת מכשירים ניידים חיונית בכך להגן על המידע שלנו מפני איומים שונים.
- ושיש, מנכ"לית חברת הייטק, השתמשה בטלפון שלה לניהול ענייני עבודה חשובים. יומ אחד, הטלפון שלה נגנב והמידע העסקתי הרגיש שנמצא בו דלף למתחרים. המידע כלל תכניות עסקיות סודיות ומודיען פיננסי, מה שגרם לנזק כלכלי ותdexתי לחברה, ופנתה היא בשאלת הרבה יניב, מה כבודו ממליץ לנו לעשות??

- ואמרתי לה שיש מספר דברים שעליה לעשות בכדי לאבטח את המ构思ור לה.

### **שיקופית 23: צעדים לאבטחת מ构思ירים ניידים:**

- 1. שימוש בסיסמאות חזקות: קביעת קוד גישה בן 6 ספרות לפחות או סיסמה חזקה לטלפון, וטוב גל להשתמש בסיסמאות מורכבות הכוללות אותיות, מספרים ותווים מיוחדים, ומומבון הגדרת קוד גישה שונה לאפליקציות רגישות כמו בנקאות ומיל.
- 2. הצפנת נתונים: טלפון המוצפן מגן על המידע שבו, הינו גם אם המ构思יר נגנב, ולכן ברוב המ构思ירים ניתן להפעיל הצפנה דרך הגדרות האבטחה, וזאת ההצפנה מגנה על הקבצים והמידע מפני גישה בלתי מורשית.
- 3. עדכוני תוכנה: גברת ריקה התקינה עדכון אבטחה שהופץ על ידי יצרן הטלפון, שסגר פרצת אבטחה חמורה, ולכן חשוב לעדכן את מערכת הפעלה והאפליקציות באופן שוטף, וחושב לדעת שעדכנים אליהם תיקוני אבטחה שמגנים מפני חולשות שהתגלו.
- 4. התקנת אפליקציות מקורות מהימנים: הורדת אפליקציות רק מחנויות רשמיות כמו App Store או Google Play וכן מומבון יש להימנע מהתקנת אפליקציות ממוקרות לא ידועים שעולות להכיל קוד זדוני, וטוב לאפשר בדיקת הרשות שהאפליקציה מבקשת לפני ההתקנה.

### **שיקופית 23: המשך צעדים לאבטחת מ构思ירים ניידים:**

- 5. שימוש באנטי-וירוס ואפליקציות אבטחה: רב חנוכה בן משה הלוי התקין אפליקציית אנטי-וירוס שמגנה על המ构思יר מפני וירוסים ותוכנות ריגול, וחושב לדעת שאפליקציות אנטי-וירוס سورחות את המ构思יר לאיתור איוימים ומסירות אותם במידה ומצאים שהוא מאיים, וכיום יש עוד אפליקציות אבטחה שיכולים להציג פיצ'רים כמו מציאת מכשיר גנוב ונעללה מרוחק.

- 6. גיבוי נתונים: כל שבוע הרב אליו מגבה את הטלפון שלו לען בכדי לשמר על המידע במקרה של אובדן המכשיר, חשוב לדעת שגיבוי קבוע של הנתונים לען או למחשב שולחני במצב של אובדן או גניבה, ניתן לשחרר את המידע בקלות.
- 7. ניהול הרשותות אפליקציות: מיכאל אוליאל בודק ומנהל את הרשותות של כל אפליקציה בטלפון שלו בכדי להבטיח שהן יונקות רק למידע שהן צרכות, וכך חשוב להבין בדיקת הרשותות אפליקציות באופן קבוע עוזר להסיר הרשותות לא נוחצות וכל זה בכדי למנוע גישה למידע רכיש.

### **שאोpit 34: שאלות על אבטחת מכשירים ניידים:**

- 1. מדוע חשוב להשתמש בסיסמאות חזקות ומורכבות במכשירים ניידים?
- 2. כיצד הצפתת המכשיר יכולה לסייע בהגנה על המידע במידה והטלפון נגנב?
- 3. מה החשיבות של התקנת עדכוני תוכנה באופן שוטף?
- 4. מדוע יש להוריד אפליקציות רק ממוקורות מהימנים?
- 5. כיצד אפליקציות אנטו וירוס יכולות להגן על המכשיר הנייד?
- 6. מה היתרון בגיבוי נתונים למכשיר נייד?
- 7. כיצד ניתן לנצל הרשותות אפליקציות במכשיר נייד ולמה זה חשוב?

### **שאोpit 35: תשובות על אבטחת מכשירים ניידים:**

- 1. סיסמאות חזקות מתקפות על תוקפים לנחש או לפצח את הקוד ולהציג גישה למכשיר ולמידע הרגיש שבו. סיסמאות מורכבות כוללות תוים שונים (אותיות, מספרים, תוים מיוחדים) ומקטיניות את הסיכוי לגישה בלתי מורשית.

- 2. הצפנה מגנה על הקבצים והמידע במכשיר כך שרק מי שיש לו את המפתח המתאים יוכל לגשת למידע. אם המכשיר נגנבו, התוקף לא יוכל לקרוא את המידע המוצפן ללא המפתח.
- 3. עדכוני תוכנה כוללים תיקוני אבטחה ופרצות שהתגלו במערכת הפעלה ובאפליקציות. התקנת עדכונים שוטפים מבטיחה שהמכשיר מוגן מפני איומים חדשים ופרצות שהתגלו.
- 4. מקורות מהימנים כמו Play Store ו-Google App מבצעים בדיקות אבטחה לאפליקציות ב כדי לוודא שאין לא מכילות קוד זדוני. הורדת אפליקציות ממוקורות לא מוכרים עלולה לחשוף את המכשיר לתוכנות זדוניות ולפרצות אבטחה.
- 5. אפליקציות אנטי וירוס סורקют את המכשיר לאיתור וירוסים ותוכנות ריגול, מסירות איומים קיימים ומספקות הגנה בזמן אמיתי מפני איומים חדשים, הם מציעות כלים נוספים כמו מציאת מכשיר גנוב ונעללה מרוחק.
- 6. Gibbs נתונים מבטיח שאם המכשיר אובד, נגנבו או ניזוק, ניתן לשחרר את המידע החשוב ולמנוע אובדן נתונים. Gibbs קבועים אפשריים ש恢 Zur מהיר של מידע בכל מצב חירום.
- 7. ניתן לנצל הרשות אפליקציות דרך הגדרות המכשיר, לבדוק אילו הרשות כל אפליקציה מבקשת ולהסיר הרשות לא נחוצות. זה חשוב כדי להבטיח שאפליקציות ניגשות רק למידע שהן צרכות, מה שungan על פרטיות המשתמש ומפחית את הסיכון לדליפת מידע.