

הרצאה 1 - אבטחת מידע וסייבר - סיכום

מסודר

מבוסס על מצגת ההרצאה (PPTX).

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

שקופית 1: הרצאה 1

שקופית 2: קורס: Information security and cyber

מרצה: יניב מורדוב

שקופית 3: מרכיבי הציון בקורס:

- מטלות ועבודות בית (ללא העתקות): 10%
- השתתפות בכיתה: 10%
- מתכונת: 70%
- התרשמות מרצה: 10%

שקופית 4: מבוא לסייבר?

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

שקופית 5: היסטוריה של סייבר

תחום הסייבר החל להתפתח בשנות ה-70 עם הופעת המחשבים האישיים והרשתות. עם השנים, ככל שהאינטרנט התפשט והמידע נעשה חשוב יותר, התפתחו גם הטכנולוגיות והאיומים הקשורים לסייבר. (נראה בהמשך דוגמאות לאיומים שהתפתחו מחמת העלייה בתוצר הטכנולוגיה)

שקופית 6: חשיבות הסייבר בעולם כיום

בעידן הדיגיטלי של היום, כל הארגונים והפרטים מסתמכים על מערכות מחשוב וניהול מידע. האיומים בעולם הסייבר כיום יכולים לגרום לנזק כלכלי עצום הבא לידי ביטוי בגניבת כסף מכספומטים (נראה בהמשך הקורס איך עושים זאת), פגיעה בפרטיות ע"י פריצה וגניבת מידע אישי (כמו תמונות לא אטיות וכו'), ואפילו להשפיע על ביטחון המדינה ע"י פריצה למערכות סופר מפוזרות שהחשיבות לשמירה בהם היא העליונה והגבוה ביותר.

שקופית 7: סוגי איומי סייבר:

- נזקות - Malware נזקה פירושה תוכנה זדונית שתפקידה להזיק למחשב או לרשת המקומית (LAN) או הציבורית (WAN). וזה כולל וירוסים, תולעים, וסוסים טרויאניים. (נראה בהמשך כל אחד בפירוט מלא עם נפקא מינות להלכה)
- התקפות פישניג - **Phishing** התקפה שבה התוקף מתחזה לגורם אמין במטרה לגנוב מידע רגיש כמו סיסמאות לכל מיני מקומות וחשבונות או פרטי אשראי. לדוגמא: 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 ובכך אנו גורמים לקריסתה ולהשבתת השירות.

- חדירות וגניבת מידע - תוקף שמצליח לחדור למערכות מחשוב ולגנוב מידע רגיש מהמשתמש כמו פרטי לקוחות, מידע כספי ועוד.

שקופית 8: דוגמאות מהעולם האמיתי:

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

שקופית 9: כלים וטכנולוגיות להגנה בסייבר

- חומות אש Firewalls - מכשירים (סנסורים) או תוכנות שמפקחים על התעבורה הנכנסת והיוצאת מהרשת ומונעים גישה בלתי מורשית.
- אנטי-וירוס וכל מיני תוכנות הגנה - תוכנות שרצות על המחשב (אפשר שיהיה באופן תמידי, אפשר עם טיימר מסוים, בדו"כ הם רצות בזמן הרצת המחשב ועם טיימר שמזוהה היא המערכת של התוכנה) וברגע שהם מזהות אזי הם מסירות את נוזקות מהמחשב.
- הצפנה Encryption - שיטה להבטחת (לשון להבטיח) סודיות המידע על ידי קידודו בצורה שלא תאפשר גישה ללא מפתח מתאים. [בהשמך הקורס נכנס ללב העיניין 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).

שקופית 10: המשך כלים וטכנולוגיות להגנה בסייבר

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

שקופית 11: עקרונות אבטחת מידע (CIA) - בסיס לאבטחת מידע

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

שקופית 12: סודיות Confidentiality

- שאלה: מה היא סודיות?
- תשובה: סודיות היא העיקרון הראשון של שמירה על פרטיות המידע כך שרק אנשים בעלי הרשאה יוכלו לגשת אליו, כלומר אנו רוצים להבטיח שמידע רגיש לא ייחשף לאנשים שאינם צריכים להיחשף.
- דוגמאות:
- הצפנת קבצים: נניח שאתה רוצה לשלוח מייל עם קובץ שמכיל מידע מסווג (כרטיס אשראי), בכדי להגן על המידע, אתה מצפין את הקובץ, מה שעושה ההצפנה היא בעצם מקודדת את המידע כך שרק מי שיש לו את המפתח המתאים יוכל לפענח ולקרוא את הקובץ.

- שימוש בסיסמאות חזקות: באתר בנק הפועלים, אתה נכנס לחשבון שלך עם שם משתמש וסיסמה. הסיסמה היא שכבת הגנה שמבטיחה שרק אתה יוכלו לגשת למידע החשבון שלך.
- אימות דו-שלבי: כדי להוסיף עוד שכבת אבטחה, ישנם אתרים הדורשים גם אימות נוסף כמו קוד שנשלח לטלפון שלך, או קוד שנשלח למייל שלך, וכל זה בנוסף לסיסמה. כך, גם אם מישהו יגלה את הסיסמה שלך, הוא עדיין יצטרך את הקוד כדי להיכנס לחשבון.

שקופית 13: שלמות Integrity

- שאלה: מה היא שלמות?
- תשובה: שלמות היא העיקרון של שמירה על כך שהמידע לא ישתנה או ייפגע על ידי גורמים שאינם מורשים. היינו רוצים להבטיח שהמידע יישאר נכון ומדויק ושלא יעשו בו שינויים שאין אנו רוצים.
- דוגמאות:
- חתימה דיגיטלית: נניח שאתה מקבל חוזה במייל, 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 שונו: בארגון גדול כמו קרית נוער בסיס הנתונים שלה הוא גדול, יש מערכות שבדקות את הנתונים בכדי לראות שהם לא נפגעו או שונו. לדוגמה, אם רשומות הלקוחות משתנות, המערכת תשלח התראה.

שקופית 14: זמינות Availability

- שאלה: מה היא זמינות?

- תשובה: זמינות היא העיקרון של הבטחת הגישה למידע ולשירותים בזמן ובמקום הרצוי, כלומר אנו רוצים לוודא שהמערכות והמידע יהיו זמינים למשתמשים המורשים בכל עת וזמן שירצו.
- דוגמאות:
- מערכות גיבוי ואחסון נתונים: חברות רבות משתמשות במערכות גיבוי כדי להבטיח שאם יש תקלה במערכת הראשית, המידע עדיין יהיה זמין. לדוגמה, אם יש בעיה במערכת השרתים, מערכת גיבוי תהיה אחראית לכך שהמידע לא יאבד ויהיה זמין לעובדים.
- התקפות מניעת שירות DDoS : כשמתקפה מסוג DDoS מנסה להפיל אתר או שירות מקוון על ידי שליחת בקשות רבות, מערכות הגנה מיוחדות מופעלות כדי לסנן את הבקשות ובכך להבטיח שהשירות יישאר זמין למשתמשים.

שקופית 15: שאלה על עיקרון CIA

- בארגון גדול, ישנה מחלקה בשם Yaniv המיישמת מדיניות אבטחת מידע מחמירה וכל זה בכדי 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 בכדי להבטיח שהמידע נשאר נכון ומדויק ולא משתנה ללא הרשאה?
- זמינות: אילו צעדים ננקטים כדי להבטיח שהמידע והשירותים יהיו זמינים למשתמשים המורשים בכל זמן שירצו?

שקופית 16: (א) תשובה - CIA

- סודיות - הארגון מיישם מערכת בקרה שמאוד מקפידה ובנוסף מבטיחה שרק עובדים מורשים יכולים לגשת למידע רגיש. כל משתמש חייב להיכנס עם שם משתמש וסיסמה ייחודיים, ולעיתים קרובות גם עם אימות דו-שלבי.
- בנוסף, המידע הרגיש מוצפן תמיד (במנוחה וגם בתנועה), כך שגם אם הפורץ מצליח להשיג גישה למערכת, הוא לא יוכלו לקרוא את המידע ללא המפתח המתאים.

שקופית 17: (ב) תשובה - CIA

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

שקופית 18: (ג) תשובה - CIA

- זמינות - הארגון מיישם מערכות גיבוי ושחזור נתונים כדי להבטיח שהמידע זמין גם במקרה של כשל במערכת הראשית. הגיבויים מתבצעים תמיד ונשמרים במקום בטוח.
- בנוסף הארגון משתמש בעוד סוגי רשתות וגם במערכת המפחיתה את העומס וזה בכדי לוודא שהשירותים יישארו זמינים גם במקרה של עליה חדה בעומס או תקלה מסוימת במערכת.

שקופית 19: גורמים שיוצרים סיכון לאבטחת מידע

הקדמה: גורמים שיוצרים לי סיכון באבטחת מידע הם הגורמים שיכולים להשפיע על הסיכון הכולל לארגון בנוגע לאבטחת המידע שלו. וחשוב מאוד להבין ולהעריך גורמים אלו לצורך זיהוי איומים, הערכת סיכונים, ותכנון השלבים הבאים המתאימות לניהול ולצמצום הסיכונים. להלן בשקופיות הבאות נראה מספר גורמי מרכיבי סיכון מרכזיים

שקופית 20: איומים Threats

- איומים הם פעולות שעלולים לגרום נזק למידע או למערכת המידע שלנו.
- דוגמאות:
- התקפות סייבר, כמו פשינג, מתקפות מניעת שירות DDoS ותוכנות זדוניות.
- גורמים פנימיים, כמו עובדים לא מרוצים, טעויות אנוש.
- גורמים טבעיים, כמו שריפות, שיטפונות, רעידות אדמה.

שקופית 21: פגיעות Vulnerabilities

- פגיעות הם חולשה במערכת כך שיכולות להיות מנוצלות על ידי איומים כדי לגרום לבאלגן.
- דוגמאות:
- חולשות תוכנה, למשל באגים, פגיעות אבטחה.
- נהלים לקויים, כמו סיסמאות חלשות, ניהול גישה לא נכון.
- תשתיות לא מאובטחות, כמו רשתות לא מוצפנות.

שקופית 22: חשיפה Exposure

- חשיפה מתארת את האפשרות שבה המידע או המערכות חשופים לאיומים ולפגיעות.
- דוגמאות:
- גישה פיזית לא מאובטחת למערכות המחשוב.
- חיבורים לא מאובטחים לרשתות חיצוניות.
- שימוש בשירותי ענן ללא אמצעי אבטחה מתאימים.

שקופית 23: השלכות Impacts

- השלכות הן התוצאה שניתן יהיה אפשר לקבל לאחר שהיה 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.

שקופית 24: גורמי מרכיבי סיכון - בתהליכים

- קודם כל נסביר מהם תהליכים (תלמדו בהמשך עם ד"ר יחזקאל גיא): תהליכים הם כללים ונהלים שהארגון מגדיר כדי לנהל ולתחזק את מערכות המידע שלו. גורמי סיכון בתהליכים נובעים מחולשות או כשלים בתהליכים אלו.
- דוגמאות:

- נהלי עבודה לא מתאימים - אם הארגון לא מגדיר נהלים ברורים לאבטחת מידע, כמו מדיניות סיסמאות חזקות או ניהול גישה למידע רגיש, ייתכן שיהיו חורים בתהליך האבטחה.
- חוסר בבקורות ותיעוד - אם לא מתעדים שינויים במערכות ולא מבצעים בקורות שוטפות, יכול להיות שלא ישימו לב לשינויים בלתי מורשים או בבעיות שנוצרות.
- תהליכי גיבוי ושחזור לא יעילים - תהליך גיבוי ושחזור לא נכון או לא מתורגל יכול לגרום לאובדן מידע קריטי בזמן חירום.

שקופית 25: גורמי מרכיבי סיכון - בטכנולוגיות

- טכנולוגיות הן הכלים שהארגון משתמש בהם וזה ביטביל לנהל ולאבטח את מערכות המידע.
- גורמי סיכון בטכנולוגיות נובעים מפגיעות במערכות או משימוש 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 תדירי, הן נשארות פגיעות לפרצות אבטחה ידועות.

שקופית 26: גורמי מרכיבי סיכון - אנושיים

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

- טעויות אנוש - עובדים יכולים בטעות להזין מידע שגוי, לשכוח לעדכן סיסמאות, או ללחוץ על קישורים זדוניים.
- חוסר מודעות - עובדים שלא מודעים לסיכונים באינטרנט עשויים ליפול למלכודות פשינג או להוריד תוכנות זדוניות (XSS).
- גורמים זדוניים פנימיים - עובדים לא מרוצים או כאלו שיש להם גישה למידע רגיש יכולים לנצל את הגישה שלהם כדי לגרום נזק מתוך נקמה למקום, או ממקום של איומים.

שקופית 27: שאלה על גורמי מרכיבי סיכון

- חברת קרית נוער החליטה לבצע הערכת סיכונים מקיפה למערכות המידע שלהם. במסגרת ההערכה, זוהו מספר פגיעות, איומים וחשיפות במערכות השונות. בהתבסס על המידע הבא, נתח את הסיכונים המוצגים והתאם לכל אחד מהם את גורמי הסיכון הרלוונטיים - תהליכים, טכנולוגיות ואנושיים.
- א. פגיעות - חוסר עדכון קבוע של מערכות הפעלה ותוכנות על שרתים. נהלי גיבוי ושחזור נתונים אינם מתורגלים באופן קבוע ואינם מתועדים כמו שצריך.
- ב. איומים - התקפות פשינג שמכוונות לעובדי הארגון, שמטרתן לגנוב אישורי גישה למערכות פנימיות. תוכנות זדוניות שמופצות ברשת הפנימית עקב הורדות בלתי מבוקרות של קבצים מהאינטרנט.
- ג. חשיפות - רשת אלחוטית פנימית שאינה מוצפנת ואינה מאובטחת כראוי. גישה פיזית בלתי מוגבלת לחדרי שרתים ואזורי עבודה מאוד מאוד רגישים.
- לאחר שקבלת את המידע הנ"ל: עליך סטודנט יקר לפרט את גורמי הסיכון המיוחסים לכל פגיעות, איומים וחשיפות. הסבר כיצד ניתן לצמצם או לנהל כל אחד מהסיכונים המוזכרים.

שקופית 28: תשובה - גורמי מרכיבי סיכון

- על בעיית - חוסר עדכון קבוע של מערכות הפעלה ותוכנות על השרתים.
- גורם סיכון - טכנולוגיות
- פתרון - יש להפעיל מצב של עדכונים אוטומטיים למערכות ההפעלה והתוכנות על השרתים.
- בנוסף יש לעקוב אחרי ההודעות על עדכוני אבטחה מיצרני התוכנה ולהתקין אותם ללא אפשרות דחיה.
- על בעיית - רשת אלחוטית פנימית שאינה מוצפנת ואינה מאובטחת.
- גורם סיכון - טכנולוגיות
- פתרון - כדאי להפעיל הצפנה חזקה על הרשת האלחוטית, ובנוסף ולהשתמש בשיטות אימות חזקות.

שקופית 29: תשובה - גורמי מרכיבי סיכון

- על בעיית - נהלי גיבוי ושחזור נתונים אינם מתורגלים ואינם מתועדים כראוי.
- גורם סיכון - תהליכים.
- פתרון - צריך לייצר נהלי גיבוי ושחזור מסודרים ולבדוק שהם מתועדים ומתורגלים באופן סדיר. זה כולל ביצוע בדיקות תקופתיות לוודא שהגיבויים מתבצעים בצורה נכונה וששחזור נתונים מתבצע כמו שצריך.

שקופית 30: תשובה - גורמי מרכיבי סיכון

- על בעיית - התקפות של פשינג שמכוונות לעובדי החברה.
- גורם סיכון - אנושיים

- פתרון - צריך לקיים הדרכות לעובדים בנוגע להתמודדות עם התקפות של פשינג, בנוסף יש

להפעיל מערכות לסינון מיילים כדי להוריד את הסיכויים שהודעות פשינג יגיעו לתיבות

למיילים של העובדים של העובדים.

הרצאה 2 - אבטחת מידע וסייבר - סיכום

מסודר

מבוסס על מצגת ההרצאה (PPTX).

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

שקופית 1: הרצאה 2

מרצה: יניב מורדוב

שקופית 2: מודל הכוכב - STAR MODEL

- טוב, אז תלמידי היקרים מהו מודל הכוכב - לא, זה לא טופולוגית כוכב של תקשוב (תשאלו את מרגי).
- מהו מודל הכוכב? מודל הכוכב הוא מודל לניהול סיכונים 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 - כמובן בהמשך תהיה דוגמא מעשית בכדי שנוכל לשכך את האוזן.

שקופית 3: ממה מורכב מודל הכוכב?

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

שקופית 4: מרכיב מודל הכוכב - אנשים

- מרכיב: אנשים People
- ביאור העיניין: האנשים בארגון הם אחד המרכיבים החשובים ביותר באבטחת מידע. הם כוללים את כל העובדים, מנהלים, ספקים ושותפים (כל מיני סוגי שותפים, והמבין יבין).
- אפשרויות שיכולות לסייע בדבר: הדרכה, מודעות, ניהול זהויות והרשאות.
- לדוגמא: קיום הדרכות באבטחת מידע וסייבר לעובדים יכול לעזור למנוע התקפות של פשינג.

שקופית 5: מרכיב מודל הכוכב - תהליכים

- מרכיב: תהליכים Processes
- ביאור העיניין: תהליכים הם הנהלים והמדיניות שמנהלים את אופן העבודה של החברה בתחום אבטחת מידע.
- אפשרויות שיכולות לסייע בדבר: מדיניות אבטחת מידע, נהלי גיבוי ושחזור, בקרת גישה.
- לדוגמא: תהליך מוגדר לשחזור מידע במקרה של תקלה כל שהיא במערכת של החברה.

שקופית 6: מרכיב מודל הכוכב - טכנולוגיה

- המרכיב: טכנולוגיה Technology
- ביאור העיניין: הטכנולוגיות הן הכלים והמכשירים שמשמשים לאבטחת מידע בארגון.
- אפשרויות שיכולות לסייע בדבר: שימוש במערכות הגנה כמו אנטי וירוס והצפנה.
- לדוגמא: התקנת תוכנות של אנטי וירוס על כל המחשבים בחברה וכל זה בכדי למנוע חדירות של תוכנות זדוניות.

שקופית 7: מרכיב מודל בכוכב - סביבה

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

שקופית 8: מרכיב מודל הכוכב - ניהול סיכונים

- מרכיב: ניהול סיכונים Risk Management
- ביאור העיניין: ניהול הסיכונים הוא תהליך של זיהוי.
- אפשרויות שיכולות לסייע בדבר: הערכת סיכונים, ניטור שוטף, תגובה לאירועים.
- לדוגמא: ביצוע הערכת סיכונים שנתית כדי לזהות ולהתמודד עם איומים חדשים.

שקופית 9: כיצד מודל הכוכב עובד?

- המודל יוצא מנקודת הנחה שהחברה צריכה להגן על הליבה שהוא בעצם 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.
- ועכשיו נראה דוגמא לדבר..

שקופית 10: דוגמא הלכה למעשה ליישום מודל הכוכב

- החברה רוצה להגן על המדע הרגיש שלה.
- מרכיב: אנשים - הדרכות תקופתיות לעובדים על נהלי אבטחת מידע, בנוסף יישום מערכת לניהול זהויות והרשאות כדי לוודא שרק אנשים מורשים יכולים לגשת למידע הרגיש.
- מרכיב: תהליכים - 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 בהצפנה למידע רגיש (וגם לכזה שלא כל כך רגיש).
- מרכיב: סביבה - התקנת מצלמות אבטחה ובקורות גישה פיזיות בחדרי שרתים ועוד, בנוסף הבטחת גישה פיזית למתקנים רק לאנשים מורשים וידועים.
- מרכיב: ניהול סיכונים - ביצוע של: הערכות, סיכונים תקופתיות, וכל זה בכדי לזהות איומים חדשים גם ישנים, בנוסף יישום מערכת לחיפוש בכל זמן ועת של פעילות רשת ואירועים חריגים.

שקופית 11: שאלה מסכמת על מודל הכוכב:

- שאלה: חברה גדולה בשם YANIV.COM רוצה להטמיע את מודל הכוכב לניהול אבטחת המידע שלו. במסגרת הטמעת המודל, נדרשת לבצע הערכה של כל אחד ממרכיבי המודל שהם: אנשים, תהליכים, טכנולוגיה, סביבה וניהול סיכונים, ולזהות אפשרויות פגיעה אפשריות.
- על הסטודנט (היינו 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.

שקופית 12: (א) תשובה - מודל הכוכב

- מרכיב: אנשים People
- פגיעה אפשרית: חוסר מודעות של העובדים לפשינג.
- דרכי התמודדות: לקיים הדרכות מודעות אבטחת מידע לעובדים על זיהוי והימנעות מהתקפות של פשינג.

שקופית 13: (ב) תשובה - מודל הכוכב

- מרכיב: תהליכים Processes
- פגיעה אפשרית: חוסר בתיקוד ובבקרת תהליכי גיבוי ושחזור.
- דרכי התמודדות: כתיבת נהלים מסודרים לגיבוי ושחזור, כך שיהיה תיעוד, ובדיקות תקופתיות בכדי שהגיבויים יתבצעו כראוי ושניתן יהיה לשחזר נתונים.

שקופית 14: (ג) תשובה - מודל הכוכב

- מרכיב: טכנולוגיה Technology
- פגיעה אפשרית: חוסר בהתקנת עדכונים וחוסר תיקונים לתוכנות.
- דרכי התמודדות: ליישם מדיניות עדכונים אוטומטיים כך שלכל המערכות והתוכנות בחברה יתבצע הדבר מאליו, ומעקב אחר עדכוני אבטחה מיצרני התוכנה.

שקופית 15: (ד)תשובה - מודל הכוכב

- מרכיב: סביבה Environment
- פגיעה אפשרית: גישה פיזית בלתי מוגבלת לחדרי שרתים ואזורי עבודה רגישים.
- דרכי התמודדות: התקנת מערכות בקרת גישה פיזית, כולל כרטיסי גישה ומצלמות אבטחה, וקביעת נהלי גישה ברורים.

שקופית 16: (ה)תשובה - מודל הכוכב

- מרכיב ניהול סיכונים Risk Management
- פגיעה אפשרית: חוסר בביצוע הערכות סיכונים תקופתיות.
- דרכי התמודדות: ביצוע הערכות סיכונים שנתיות לזיהוי איומים חדשים ויישום מערכות לחיפוש תמידי לאירועים לא רגילים.

שקופית 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 ואבטחה. הרעיון המרכזי במודל הוא שבמקום 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. אבטחה פיזית
 2. אבטחת רשת
 3. אבטחת היקף

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

שקופית 18: שכבה 1 של Depth in Defense

- שכבה : אבטחה פיזית - Physical Security
- ביאור העיניין: אבטחה פיזית מתייחסת להגנה על החומרה והמכשירים עצמם מפני גישה בלתי מורשית, גניבה או נזק פיזי.
- לדוגמא: שימוש במנעולים, כרטיסי גישה, מצלמות אבטחה ושומרים.

שקופית 19: שכבה 2 של Depth in Defense

- שכבה: אבטחת רשת - Network Security
- ביאור העיניין: אבטחת רשת מתמקדת בהגנה על תעבורת הרשת ועל המידע המועבר ברשת מפני התקפות וחדירות.
- לדוגמא: פיירוולים, מערכות זיהוי ומניעת חדירות IDS/IPS הצפנת תעבורה באמצעות VPN

שקופית 20: שכבה 3 של Depth in Defense

- שכבה: אבטחת היקף - Perimeter Security

- ביאור העיניין: להגן על הגבולות החיצוניים של הרשת כדי למנוע חדירה ראשונית של גורמים עוינים.
- לדוגמא: פיירוולים היקפיים, סינון דוא"ל, סינון אתרים, שערי רשת.

שקופית 21: שכבה 4 של Depth in Defense

- שכבה: אבטחת נקודות קצה - Endpoint Security
- ביאור העיניין: להגן על המכשירים המחוברים לרשת כמו מחשבים, סרברים, פאלפונים חכמים ועוד - מפני התקפות.
- לדוגמא: אנטי וירוס, אנטי תוכנה זדונית.

שקופית 22: שכבה 5 של Depth in Defense

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

שקופית 23: שכבה 6 של Depth in Defense

- שכבה: אבטחת נתונים - Data Security

- ביאור העיניין: להגן על הנתונים עצמם, בין אם במנוחה או בתנועה היינו בשימוש - מפני גישה בלתי מורשית, שינוי או הריסה הרמטית.
- לדוגמא: הצפנת נתונים, גיבויים.

שקופית 24: שכבה 7 של Depth in Defense

- שכבה: מדיניות, נהלים ומודעות - Policies, Procedures, and Awareness
- ביאור העיניין: להגדיר את המדיניות והנהלים הנחוצים לשמירה על המידע שלי, ובנוסף להגביר את המודעות של העובדים לנושאי אבטחת המידע בחברה.
- לדוגמא: כתיבת מדיניות אבטחת מידע, הדרכות לעובדים, ובקרת נתונים.

שקופית 25: שאלה מסכמת על Depth in Defense

שאלה: בחברת ELIRAN_SHUDED_ZKENUT.COM מיושמת גישת Depth in Defense להגנה על מערכות המידע שלהם. החברה סובלת מהתקפות חוזרות על היישומים השונים שלה, המנוצלות על ידי האקרים, וכל זה בכדי לגנוב נתונים אישיים. באילו שכבות של מודל Depth in Defense על החברה להתמקד כדי לטפל בבעיה הזאת, ובאלה צעדים מעשים צריכים לנקוט בכל שכבה ושכבה?

שקופית 26: תשובה

- עלינו להתמקד ב-3 שכבות והם: אבטחת יישומים, אבטחת נתונים, ומדיניות נהלים ומודעות.

- 1. אבטחת יישומים: לבצע בדיקות חדירות ליישומים בכדי לזהות ולתקן פרצות אבטחה, בנוסף יש להשתמש ב-WAF בכדי 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 בכלים לבדיקת קוד בזמן הפיתוח.
- 2. אבטחת נתונים: הצפנת נתונים רגישים הן בזמן שמירתם והן בזמן שליחתם, ובנוסף לבצע גיבויים סדירים של הנתונים ולשמור אותם במקום בטוח. ואפשר גם יישום בקרת גישה מבוססת תפקידים בכדי להגביל את הגישה לנתונים רק לאנשים ספציפיים ולא לכולם.
- 3. מדיניות נהלים ומודעות: כתיבת מדיניות אבטחת מידע שמגדירה את הדרישות להגנה על יישומים ונתונים וגם כדאי לעשות הדרכות לעובדים בנושא אבטחת יישומים ונתונים בכדי להעלות את המודעות לסיכונים ולדעת כיצד מגנים, וצריך גם לבצע ביקורת סדירה על היישומים והנתונים בכדי להבטיח עמידה במדיניות ובנהלים.

הרצאה 3 - אבטחת מידע וסייבר - סיכום

מסודר

מבוסס על מצגת ההרצאה (PPTX).

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

שקופית 1: הרצאה 3

מרצה: יניב מורדוב

שקופית 2: אבטחת תשתיות מחשב

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

שקופית 3: אבטחה על מחשב בודד

- אבטחת מחשב בודד מחולקת להרבה תחומים ואלו הן:
- 1. התקנת מערכת הפעלה מאובטחת - התקן מערכת הפעלה מעודכנת ונתמכת כמו: Linux, Windows 10 וגם צריך לבדוק שהמערכת מעודכנת עם כל העדכונים האחרונים.
- 2. הגנה באמצעות סיסמא - 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, בכדי להגן על המחשב מפני וירוסים ותוכנות זדוניות וטוב גם לבדוק שהתוכנה מעודכנת ומתבצעות סריקות כל פרק זמן מסוים.

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

שקופית 4: המשך דרכי אבטחה על מחשב בודד

- 6. גיבויים - יש לבצע גיבויים סדירים של הנתונים החשובים במחשב, וגם לשמור גיבויים במיקום בטוח ונפרד מהמחשב לדוגמא: כונן חיצוני או שירות ענן.
- 7. עדכוני תוכנה - לבדוק שכל התוכנות המותקנות במחשב מעודכנות לגרסה האחרונה, ובנוסף יש להפעיל עדכונים אוטומטיים בכדי לקבל את כל התיקונים והעדכונים הנדרשים בזמנם.
- 8. מודעות והדרכה - ללמד את המשתמשים על נהלי אבטחה, כמו זיהוי פישונג, אי פתיחת קבצים מצורפים לא מזוהים, ולא להוריד תוכנות ממקורות לא אמינים.
- 9. הרשאות וגישה - להגדיר הרשאות גישה מתאימות לכל המשתמשים במחשב, היינו להשתמש בחשבונות משתמש עם הרשאות מוגבלות לעבודה, והשתמש בחשבון מנהל רק כאשר יש צורך בכך.
- 10. ניטור ותגובה לאיומים - להתקין כלי בכדי לעקוב אחרי פעולות חשודות במחשב, וגם תתכונן להגיב לאירועי אבטחה במהירות.

שקופית 5: אבטחת חומרה

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

שקופית 6: כיצד לאבטח חומרה?

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

שקופית 7: אבטחת קושחה

מה היא קושחה? קושחה Firmware היא התוכנה המובנית בתוך רכיבי החומרה, כמו ה-BIOS או ה-UEFI בלוח האם, תוכנת הבקרה במעבדים, בקרי רשת, ועוד. אבטחת קושחה תפקידה בהגנה על תוכנה זו מפני התקפות שעלולות לשנות את פעולתה או לנצל פרצות אבטחה שבה הוכחה מחישוביות.

שקופית 8: כיצד לאבטח קושחה

- 1. עדכוני קושחה - התקנת עדכוני קושחה מיצרן החומרה כדי לתקן פרצות אבטחה שהתגלו לאחר זמן, ובנוסף בדיקה תקופתית של עדכונים חדשים והתקנתם באופן תדיר.
- 2. הגנה על BIOS, UEFI - להגדיר סיסמא להגנה על ה-BIOS, UEFI בכדי למנוע גישה לבלתי מורשים.
- 3. הצפנה ואימות - לינתן להשתמש בטכנולוגיות הצפנה ואימות בקושחה בכדי למנוע שינוי בלתי מורשה או הזרקת קוד זדוני INJECTION וגם לבדוק שהקושחה חתומה דיגיטלית בעת התקנתה.
- 4. גיבוי ושחזור - גיבוי הקושחה חשובה כדי לאפשר שחזור במקרה של תקלה או שינוי של התוקף, וכמובן שמירה על גיבויים במיקום מאובטח ונפרד מהמחשב.
- 5. ניטור פעילות חריגה - להתקין כלי חיפוש לזיהוי פעילות חריגה בקושחה, כגון שינוי בלתי מורשה בהגדרות ה-BIOS, UEFI.

שקופית 9: * (למעוניינים) במידה ואתם שמים סיסמה ב-BIOS:

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

שקופית 10: שאלה על אבטחת חומרה וקושחה:

- שאלה: חברת תוכנה בשם DANIEL.COM החליטה להקשיח את מערך המחשוב שלה בעקבות מתקפות סייבר חוזרות ונישנות. כחלק מהתהליך, החברה רוצה להבטיח שאף אחד לא יוכל לשנות את הגדרות ה- BIOS או להעלות מערכת הפעלה לא מאומתת.
- 1. הסבר כיצד ניתן להגן על הגדרות ה-BIOS/UEFI מפני גישה בלתי מורשית?
- 2. וגם מדוע חשוב להפעיל אפשרות של Secure Boot ?

שקופית 11: תש בה:

- 1. הגדרת סיסמה ל-BIOS/UEFI : כדי להגן על הגדרות ה-BIOS/UEFI יש להגדיר סיסמת מנהל מערכת Administrator Password ואנו צריכים סיסמה זו בכדי לגשת ולשנות את הגדרות ה-BIOS/UEFI. ובנוסף ניתן להגדיר סיסמת משתמש שתידרש בעת אתחול המחשב, כך שרק מי שמכיר את הסיסמה יוכל לאתחל את המחשב.
- 2. Secure Boot מוודא שרק תוכנות מערכת הפעלה מאומתות וחתומות דיגיטלית על ידי היצרן ייטענו במהלך אתחול המחשב ולא דברים אחרים. ובנוסף זה מונע מתוכנות זדוניות להיטען ולהשיג 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 קריטיות במערכת.

שקופית 12: הקשחת מערכת ההפעלה

- מהי הקשחת מערכת ההפעלה?

- הקשחת מערכת ההפעלה (OSH) Operating System Hardening היא תהליך של חיזוק ההגנות והקטנת הפגיעות של מערכת ההפעלה מפני התקפות וסיכונים. תפקידנו להפחית את מספר הנקודות הפגיעות שבמערכת שיכולות להיות מנוצלות על ידי תוקפים ובכך להבטיח שמערכת ההפעלה תהיה כמה שיותר מאובטחת ולא פגיעה.

שקופית 13: השלבים להקשחת מערכת ההפעלה:

- 1. עדכונים ותיקונים Patching: צריכים אנו לוודאות שכל העדכונים והתיקונים האחרונים של מערכת ההפעלה מותקנים אצלנו, ובנוסף הפעל עדכונים אוטומטיים כדי לקבל תיקונים חדשים באופן עכשווי.
- 2. הגדרות אבטחה Security Settings: עדכן את הגדרות האבטחה המובנות של מערכת ההפעלה, וגם תוודא שהגדרות האבטחה המומלצות מיושמות.
- 3. הגנה על חשבונות משתמש: השתמש בסיסמאות חזקות לכל החשבונות, וטוב גם להשתמש באימות דו שלבי עבור חשבונות המשתמשים.
- 4. כיבוי שירותים ותכונות לא נחוצים: נטרל שירותים ותכונות שלא בשימוש בכדי לצמצם את שטח התקיפה.
- 5. פיירוול Firewall: הפעל את הפיירוול המובנה במערכת ההפעלה, ובנוסף הגדר כללים מגבילים לגישה מרשתות חיצוניות.
- 6. אנטי-וירוס ואנטי תוכנה זדונית: התקן תוכנות אנטי-וירוס ואנטי-תוכנה זדונית, ובנוסף תודא שהתוכנות מעודכנות ומתבצעות סריקות בצורה תדירית.

שקופית 14: המשך- שלבים להקשחת מערכת ההפעלה

- 7. הצפנה: הצפן את הכונן הקשיח באמצעות BitLocker ב-Windows (וכל מערכת ההפעלה ההצפנה תהיה ע"י תוכנה שונה), ובנוסף השתמש בהצפנת קבצים עבור נתונים רגילים.
- 8. ניהול עדיפויות Permissions Management - הגבל את הגישה לקבצים ותיקיות רגילות, ובנוסף הגדר הרשאות גישה מתאימות למשתמשים ולתוכנות ספציפיות.
- 9. הגנה על רשת: השתמש ב-VPN לגישה מרחוק, ובנוסף תודא שמכשירים מחוברים לרשת מאובטחת.
- 10. ניטור ובקרה: התקן כלי ניטור לזיהוי פעילות חריגה, ובנוסף הקם מערכת התראות להתראה מיידית על אירועי אבטחה.
- 11. בקרת גישה: השתמש ב-Access Control Lists (ACLs) לניהול גישה לקבצים ותיקיות.

שקופית 15: שאלה על הקשחת מערכת ההפעלה:

מסוימת מנסה באופן חוזר לגשת למערכת שלך ומציגה התנהגות חשודה. כדי IP שאלה: כתובת זו באמצעות פיירוול. IP להקשיח את מערכת ההפעלה שלך, עליך לחסום את הגישה מכתובת כדי לחסום iptables-המשתמש ב] עבור מערכת הפעלה לינוקס Bash -כתוב סקריפט פשוט ב [192.168.1.100-IP את הגישה מכתובת ה

```
IP_TO_BLOCK="192.168.1.100"
```

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

- # שמירת החוקים כך שישרדו אתחול מחדש של המערכת

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

- אנחנו רוצים לחסום את הכתובת הנ"ל, ואנו נציב אותה במשתנה, ומיד אח"כ אנו משתמשים בפקודה בכדי לחסום את הכתובת הנ"ל וכמובן גם כל תנועה מאותה הכתובת אנו חוסמים, אנו ניגע בפקודות הללו שנגיע לפירוול
- אנחנו משתמשים בפקודת את התנועה מכתובת ה-IP.

שקופית 16: שאלה עיונית - דומה לשאלות בחינה סופית

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

שקופית 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 המערכות, הוא שם לב שחלק מהמחשבים מריצים יישומים שונים בהרשאות מנהל, בעקבות כך יוסי החליט לבצע הקשחת מערכת ההפעלה כדי להגן על המחשבים והשרתים של החברה.

- כחלק מהפעולות להקשחת מערכת ההפעלה, יוסי החליט להפעיל את מנגנון ה-UAC (בקרה על המשתמשים) במחשבי החברה. הסבר מהו מנגנון ה-UAC וכיצד הוא תורם להקשחת מערכת ההפעלה ולהגנה מפני תוכנות זדוניות.

שקופית 18: תש בה:

- מנגנון ה-UAC (User Account Control) הוא תכונת אבטחה במערכות הפעלה Windows שמטרתה להגביל את ההרשאות של תוכנות ומשתמשים, על מנת להפחית את הסיכון לנזקים ממקור תוכנות זדוניות ושגיאות משתמש.
- ה-UAC תורם להקשחת מערכת ההפעלה ולהגנה מפני תוכנות זדוניות על ידי:
 1. בקרת הרשאות: UAC דורש אישור מהמשתמש לפני הרצת יישומים שדורשים הרשאות מנהל, מה שמקשה על תוכנות זדוניות לבצע פעולות מזיקות ללא ידיעת המשתמש.
 2. הרצת יישומים בהרשאות מוגבלות: כברירת מחדל, יישומים רצים בהרשאות משתמש רגיל, וההרשאות מוגבלות מורידות את הסיכון לניצול פרצות בתוכנה.
 3. מניעת התקנות לא מורשות: UAC מקשה על התקנת תוכנות חדשות ללא אישור מפורש של המשתמש עם הרשאות מתאימות.

שקופית 19: הקשחת רכיבי תקשורת

- חברת YANIC.COM היא חברת טכנולוגיה עם משרדים רבים ברחבי העולם. יום אחד, צוות האבטחה גילה שיש תנועה בלתי רגילה ברשת החברה. חקירה מהירה העלתה ששרתים רבים במשרד המרכזי החלו לשלוח נתונים גדולים לכתובת IP זרה.

- צוות האבטחה הבין במהירות שמדובר בפריצה רצינית, והחל בניתוח האירוע. הסתבר שתוקפים הצליחו לפרוץ לנתב מרכזי שהיה מוגדר עם סיסמת ברירת מחדל. לאחר הפריצה, התוקפים יכלו להקשיב לכל התעבורה ברשת ולשלוט בה.
- ובגלל הבעיה בנתב, שהנתב הינו רכיב תקשורת אנו צריכים להקשיח.

שקופית 20: כיצד מקשיחים רכיבי תקשורת:

- 1. שינוי סיסמאות ברירת מחדל: במקרים רבים, תוקפים מצליחים לחדור לרשתות פשוט על ידי שימוש בסיסמאות ברירת מחדל של רכיבי הרשת. לדוגמה, תוקף שהצליח להיכנס למתג רשת במפעל גדול, הצליח להשתלט על כל תעבורת הרשת פשוט על ידי כניסה עם סיסמת ברירת המחדל.
- אז מה עושים? יש לשנות את סיסמאות ברירת המחדל של כל רכיבי התקשורת לסיסמאות חזקות וייחודיות מיד עם התקנתם.
- 2. עדכוני תוכנה וקושחה Firmware: בשנת 2018, פרצה נחשפה בקושחת נתב פופולרי, שמאפשרת לתוקפים להשתלט על הנתב מרחוק. התקפות רבות ניצלו את הפרצה עד שיצרן הנתב פרסם עדכון קושחה שתיקן את הבעיה.
- אז מה עושים? יש לעדכן את הקושחה והתוכנה של רכיבי התקשורת באופן קבוע. עדכונים אלו כוללים לעיתים קרובות תיקוני אבטחה לחולשות שהתגלו.
- 3. ניהול גישה והרשאות: חברת ייעוץ גלובלית גילתה שתוקף הצליח להשתלט על חשבון מנהל מערכת של מתגי הרשת התוקף השיג גישה דרך חשבון עם הרשאות גבוהות שלא היה צריך להיות פעיל.
- אז מה עושים? יש להגדיר הרשאות מינימליות Least Privilege לכל משתמש ויישום, ולוודא שרק מי שצריך גישה יקבל אותה.

שקופית 21: המשך הקשחת רכיבי תקשורת:

- 4. הגבלת גישה מרחוק: במתקפה על בנק מקומי, התוקפים השתמשו בפרוטוקול Telnet כדי לגשת לנתבים ולשנות את הגדרותיהם, מה שאיפשר להם ליירט תעבורה ולגנוב נתונים רגישים.
- מה עלינו לעשות? יש להגביל את הגישה מרחוק לרכיבי הרשת ולהשתמש בשיטות גישה מאובטחות כמו VPN ו-SSH במקום פרוטוקולים פחות מאובטחים כמו Telnet.
- 5. שימוש בפרוטוקולי תקשורת מאובטחים: ארגון רפואי גילה שהתקפות MITM (Man-in-the-Middle) מתבצעות על התקשורת שלהם, משום שהם השתמשו בפרוטוקול HTTP לא מוצפן לשליחת נתונים בין שרתים.
- מה עלינו לעשות? יש להשתמש בפרוטוקולים מאובטחים כמו HTTPS במקום HTTP, ו-SNMPv3 במקום גרסאות ישנות יותר של SNMP.
- 6. יישום בקורות גישה מבוססות כתובת IP (ACLs): חברת לוגיסטיקה הצליחה למנוע מתקפת סייבר כשהשתמשו ב-ACLs כדי לחסום תעבורה חשודה מכתובות IP זרות שזוהו בניסיונות גישה לא מורשים.
- ולכן יש להגדיר ACLs כך שיגבילו את הגישה לרכיבי הרשת על פי כתובות IP מאושרות בלבד.
- 7. ניטור והתרעה: בית חולים גילה מתקפה על מערכתיו רק לאחר שהמערכות התריעו על תעבורה חריגה לשרתים חיצוניים בשעות הלילה. בזכות מערכות הניטור, הצליחו להפסיק את ההתקפה בזמן.
- ולכן טוב מאוד להטמיע מערכות לניטור והתרעה SIEM שיתריעו על פעילות חריגה ויאפשרו תגובה מהירה לאירועים חשודים.
- 8. פיצול רשת: חברת ייצור הצליחה לצמצם את הנזק מהתקפת כופרה (vlan) Ransomware על ידי פיצול הרשת שלה כך שההתקפה לא יכלה להתפשט למקטעים קריטיים אחרים של הרשת.

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

שקופית 22: שאלה

- בחברת ELIRAN_AND_DANIEL עבד צוות IT שהשקיע רבות באבטחת הרשת. יום אחד, המנכ"ל קיבל דוא"ל אנונימי שטען כי מערכת הרשת של החברה פגיעה וחשופה לתקיפות. הדוא"ל הכיל פרטים על מספר רכיבי תקשורת שהיו בשימוש החברה עם סיסמאות ברירת מחדל.
- יניב הוא מנהל אבטחת המידע הוא גילה שמתגי הרשת במשרדים הראשיים עדיין השתמשו בסיסמאות ברירת מחדל שהיו ידועות לכל. יניב הבין שעליו להקשיח את רכיבי התקשורת בצורה מיידית!!
- תן 5 הצעדים העיקריים שיניב יכול לנקוט להקשחת רכיבי התקשורת של החברה, וכיצד שינוי סיסמאות ברירת מחדל יכול למנוע התקפות בעתיד?

שקופית 23: תשובה

- 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 התקשורת לסיסמאות חזקות וייחודיות. פעולה זו תמנע מתוקפים להשתמש בסיסמאות ידועות כדי לגשת לרכיבים.
- 2. עדכוני תוכנה וקושחה: יש לוודא שכל רכיבי התקשורת מעודכנים לגרסאות התוכנה והקושחה האחרונות, אשר כוללות תיקוני אבטחה לחולשות שהתגלו.

- 3. ניהול גישה והרשאות: הגדרת הרשאות מינימליות למשתמשים ורכיבים כך שכל משתמש יקבל גישה רק למשאבים הנחוצים לו.
- 4. הגבלת גישה מרחוק: שימוש בשיטות גישה מאובטחות כמו VPN ו-Ssh במקום פרוטוקולים פחות מאובטחים כמו Telnet והגבלת הגישה מרחוק רק למשתמשים מורשים.
- 5. שימוש בפרוטוקולי תקשורת מאובטחים: יש להפעיל פרוטוקולים מאובטחים כמו HTTPS ו-SNMPv3 על רכיבי התקשורת.
- 6. ועוד..
- * וחשוב להדגיש ששינוי סיסמאות ברירת מחדל לרכיבי התקשורת הוא קריטי משום שסיסמאות ברירת מחדל ידועות לציבור ויכולות לשמש תוקפים לגישה לא מורשית לרשת. על ידי שינוי הסיסמאות, יניב מצמצם את הסיכון להתרחשות התקפות נוספות.

שקופית 24: כלי חשוב שראינו לעיל

כדי להגן על הרשת ניתן להשתמש בפקודה הזאת בכדי לחסום את כל התנועה - iptables
הזו IP-הנכנסת מכתובת ה

`sudo iptables -A INPUT -s 192.168.1.100 -j DROP`: לדוגמא

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

שקופית 25: הקשחת 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 OAR.jERUSALEM.tOAR היא ספקית שירותים המחזיקה מסדי נתונים עם מידע רגיש של לקוחותיה. באחד הימים, תוקף הצליח לחדור למערכת החברה באמצעות מתקפת SQL Injection (שאותה נלמד לבצע בהמשך הקורס) בה הוא הזריק פקודות זדוניות לטופס חיפוש באתר החברה. דרך כך, התוקף השיג גישה בלתי מורשית למידע של אלפי לקוחות.
- ולכן מחמת הבעיה הזאת אנו צריכים להקשיח את מסדי הנתונים שלנו.

שקופית 26: מה עלינו לעשות בהקשחת מסדי הנתונים:

- 1. אימות וניהול משתמשים: בחברת YANIV.COM חשבון מנהל מסד נתונים היה מוגדר ללא סיסמה חזקה, ותוקף הצליח לנחש את הסיסמה ולגשת למידע הרגיש.
- הקשחה: שימוש בסיסמאות חזקות ומורכבות לכל המשתמשים, וגם הטמעת אימות דו-שלבי לגישה למסד הנתונים, ובנוסף הקצאת הרשאות מינימליות על פי תפקיד המשתמש.
- 2. חברת אינטל איבדה מחשב נייד שכלל גיבוי של מסד נתונים עם מידע רפואי רגיש שלא היה מוצפן. המידע נגנב והדליף לציבור.
- הקשחה: הצפנת נתונים במנוחה ובתנועה וכל זה בכדי להגן על מידע רגיש, ובנוסף שימוש בתעודות SSL/TLS להבטחת תקשורת מוצפנת בין השרתים והלקוחות.
- 3. הגנה מפני SQL Injection: חברת CISCO נפגעה ממתקפת SQL Injection שחשפה את פרטי הלקוחות שלה. המתקפה התבצעה על ידי הזרקת פקודות SQL זדוניות לטפסי הזמנות מקוונים.

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

שקופית 27: המשך - מה עלינו לעשות בהקשחת מסדי הנתונים:

- 4. ניהול עדכונים וטלאי אבטחה: בחברת ELIRAN.COM מסדי הנתונים לא עודכן לגרסה האחרונה, ונמצאה בו חולשת אבטחה קריטית. תוקפים ניצלו את החולשה לגנוב מידע של סטודנטים.
- הקשחה: עדכון שוטף של גרסאות מסדי הנתונים והטמעת טלאי אבטחה ובנוסף שימוש בתהליכי CI/CD לבדיקת אבטחה ויישום עדכונים באופן מתמיד.
- 5. גיבוי ושחזור נתונים: חברת ULIEL.CO.IL חוותה מתקפת שבה הושבתו מסדי הנתונים שלה. בגלל שלא היו גיבויים עדכניים, החברה איבדה נתונים קריטיים והייתה צריכה לשלם כופר גבוה.
- הקשחה: גיבוי נתונים באופן קבוע ושמירת גיבויים במיקום מאובטח. בדיקה תקופתית של תהליך השחזור כדי לוודא שניתן לשחזר את הנתונים במהירות במקרה של איבוד נתונים.
- 6. ניטור והתרעה: חברת NOAN.AC הצליחה למנוע גניבת מידע לאחר שמערכות הניטור שלה זיהו פעילות חשודה במסדי הנתונים. התוקף ניסה לשאוב כמות גדולה של נתונים בצורה לא רגילה.
- הקשחה: הטמעת מערכות ניטור והתרעה SIEM לניטור תעבורת מסדי הנתונים וזיהוי פעילות חריגה, ובנוסף צריך לעשות ניתוח לוגי בכדי לזהות ולהגיב במהירות לאירועי אבטחה.

שקופית 28: שאלות על הקשחת מסדי נתונים:

- 1. מה היתרונות של שימוש באימות דו שלבי במסדי נתונים?
- 2. מהי מתקפת SQL Injection וכיצד 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 ומניעת מתקפות על מסדי נתונים?

שקופית 29: תשובות על הקשחת מדי 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 משיגים את הסיסמה בגלל שהם עדיין זקוקים לאותו פריט נוסף.
- 2. מתקפת SQL Injection מתרחשת כאשר תוקף מחדיר פקודות SQL זדוניות לתוך שאילתה של מסד הנתונים דרך קלט משתמש לא מסונן. ולכן ניתן למנוע מתקפות כאלה על ידי שימוש בפרמטרים בשאילתות Prepared Statements או על ידי הטמעת ספריות ORM (Object-Relational Mapping) שמטפלות באבטחת השאילתות באופן אוטומטי.
- 3. עדכונים וטלאי אבטחה כוללים תיקונים לחולשות שהתגלו בגרסאות קודמות. השארת מערכת לא מעודכנת חושפת את המערכת לסיכונים והתקפות שעלולות 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 תהליך השחזור כדי לוודא שהוא פועל כראוי, ולהיות מוכנים עם תוכנית שחזור שמפרטת את הצעדים לשחזור הנתונים במקרה של איבוד.

- 5. מערכות SIEM (Security Information and Event Management) מנטרות את התעבורה והפעילות במסד הנתונים, מנתחות לוגי וגם מזהות פעילות חריגה או חשודה בנוסף הם יכולות לשלוח התרעות בזמן אמת ולהפעיל תהליכים אוטומטיים לטיפול באירועי אבטחה, ובכך לסייע במניעת מתקפות או זיהוי מוקדם שלהן.

שקופית 30: דוגמא של קוד המונע SQL Injection

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

- השתמשנו בפרמטרים בכדי למנוע SQL Injection וע"י הפקודה הנ"ל מקבלת השאילתה את הפרמטרים כטאפלים, מה שמונע הזרקת SQL.
- הבשמך אנו נלמד בעיון איך וכיצד מזריקים – אל תדאגו הכל יהיה בסדר

שקופית 31: אבטחת מכשירים ניידים

- פתיחה לחכמה: מכשירים ניידים כמו טלפונים חכמים וטאבלטים הם חלק בלתי נפרד מחיינו. אנו משתמשים בהם לאחסון מידע אישי ועסקי רגיש, מה שמעמיד אותם כיעד מרכזי למתקפות סייבר. אבטחת מכשירים ניידים חיונית בכדי להגן על המידע שלנו מפני איומים שונים.
- שויש, מנכ"לית חברת הייטק, השתמשה בטלפון שלה לניהול ענייני עבודה חשובים. יום אחד, הטלפון שלה נגנב והמידע העסקי הרגיש שנמצא בו דלף למתחרים. המידע כלל תכניות עסקיות סודיות ומידע פיננסי, מה שגרם לנזק כלכלי ותדמיתי לחברה, ופנתה היא בשאלה לרב יניב, מה כבודו ממליץ לנו לעשות??

- ואמרתי לה שיש מספר דברים שעליה לעשות בכדי לאבטח את המכשיר לה.

שקופית 32: צעדים לאבטחת מכשירים 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, וכמובן הגדרת קוד גישה שונה לאפליקציות רגישות כמו בנקאות ומייל.
- 2. הצפנת נתונים: טלפון המוצפן מגן על המידע שבו, היינו גם אם המכשיר נגנב, ולכן ברוב המכשירים 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 ההפעלה והאפליקציות באופן שוטף, וחשוב לדעת שעדכונים אלו כוללים תיקוני אבטחה שמגנים מפני חולשות שהתגלו.
- 4. התקנת אפליקציות ממקורות מהימנים: הורדת אפליקציות רק מחנויות רשמיות כמו Google Play או App Store וכמובן יש להימנע מהתקנת אפליקציות ממקורות לא ידועים שעלולות להכיל קוד זדוני, וטוב לאפשר בדיקת הרשאות שהאפליקציה מבקשת לפני ההתקנה.

שקופית 33: המשך צעדים לאבטחת מכשירים ניידים:

- 5. שימוש באנטי-וירוס ואפליקציות אבטחה: רבי חנוכה בן משה הלוי התקין אפליקציית אנטי וירוס שמגנה על המכשיר מפני וירוסים ותוכנות ריגול, חושב לדעת שאפליקציות אנטי וירוס סורקות את המכשיר לאיתור איומים ומסירות אותם במידה ומוצאים משהו מאיים, וכיום יש עוד אפליקציות אבטחה שיכולות להציע פיצ'רים כמו מציאת מכשיר גנוב ונעילה מרחוק.

- 6. גיבוי נתונים: כל שבוע הרב אלי מגבה את הטלפון שלו לענן בכדי לשמור על המידע במקרה של אובדן המכשיר, חשוב לדעת שגיבוי קבוע של הנתונים לענן או למחשב שולחני במצב של אובדן או גניבה, ניתן לשחזר את המידע בקלות.
- 7. ניהול הרשאות אפליקציות: מיכאל אוליאל בודק ומנהל את ההרשאות של כל אפליקציה בטלפון שלו בכדי להבטיח שהן ניגשות רק למידע שהן צריכות, ולכן חשוב להבין בדיקת הרשאות אפליקציות באופן קבוע עוזר להסיר הרשאות לא נחוצות וכל זה בכדי למנוע גישה למידע רגיש.

שקופית 34: שאלות על אבטחת מכשירים ניידים:

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

שקופית 35: תשובות על אבטחת מכשירים ניידים:

- 1. סיסמאות חזקות מקשות על תוקפים לנחש או לפצח את הקוד ולהשיג גישה למכשיר ולמידע הרגיש שבו. סיסמאות מורכבות כוללות תווים שונים (אותיות, מספרים, תווים מיוחדים) ומקטינות את הסיכוי לגישה בלתי מורשית.

- 2. הצפנה מגנה על הקבצים והמידע במכשיר כך שרק מי שיש לו את המפתח המתאים יכול לגשת למידע. אם המכשיר נגנב, התוקף לא יוכל לקרוא את המידע המוצפן ללא המפתח.
- 3. עדכוני תוכנה כוללים תיקוני אבטחה ופרצות שהתגלו במערכת ההפעלה ובאפליקציות. התקנת עדכונים שוטפים מבטיחה שהמכשיר מוגן מפני איומים חדשים ופרצות שהתגלו.
- 4. מקורות מהימנים כמו Google Play ו-App Store מבצעים בדיקות אבטחה לאפליקציות בכדי לוודא שהן לא מכילות קוד זדוני. הורדת אפליקציות ממקורות לא מוכרים עלולה לחשוף את המכשיר לתוכנות זדוניות ולפרצות אבטחה.
- 5. אפליקציות אנטי וירוס סורקות את המכשיר לאיתור וירוסים ותוכנות ריגול, מסירות איומים קיימים ומספקות הגנה בזמן אמת מפני איומים חדשים, הם מציעות כלים נוספים כמו מציאת מכשיר גנוב ונעילה מרחוק.
- 6. גיבוי נתונים מבטיח שאם המכשיר אובד, נגנב או ניזוק, ניתן לשחזר את המידע החשוב ולמנוע אובדן נתונים. גיבויים קבועים מאפשרים שחזור מהיר של מידע בכל מצב חירום.
- 7. ניתן לנהל הרשאות אפליקציות דרך הגדרות המכשיר, לבדוק אילו הרשאות כל אפליקציה מבקשת ולהסיר הרשאות לא נחוצות. זה חשוב כדי להבטיח שאפליקציות ניגשות רק למידע שהן צריכות, מה שמגן על פרטיות המשתמש ומפחית את הסיכון לדליפת מידע.