"רשת ביטחון"

אוגדן ניתוחי אירוע

אירוע 1- הדלפה בפלטפורמת Polymarket

<u>תקציר האירוע:</u>

פלטפורמת Polymarket הינה פלטפורמה דיגיטלית להערכת הסתברויות של מגוון רחב של אירועים עתידיים במגוון תחומים – מזג אוויר, ביטחון, פוליטיקה, משחקי ספורט וכו'.

התשתית פועלת במרחב השחור תוך שימוש במטבעות קריפטוגרפים, ובמסגרתה המשתמשים יכולים להצביע "כן" או "לא" לתרחישים השונים שעולים לפלטפורמה, כאשר ההסתברות ל"זכייה" (מהימנות והתממשות התרחיש) משתקפת במחיר "מניה", והיא מושפעת בזמן אמת מהיקף הפעילות והסכומים שהושקעו.

ברקע באותה תקופה - היערכות וכוננות צה"לית גבוהה הקשורה במערכה אל מול איראן ותכנון תקיפה ישראלית, במהלכה התגלה כי אזרח ומספר משרתי מילואים בחה"א השתמשו בפלטפורמה לטובת רווח אישי והימרו על מועדי תקיפת צה"ל באיראן.

במסגרת חקירת האירוע, התגלה כי ההימורים שבוצעו נעשו על סמך מידע מסווג אליו אנשי המילואים נחשפו במסגרת תפקידם, ולעיתים אף בזמן אמת הסמוך למימוש תקיפות ופעולות קינטיות אחרות.

המעורבים הרוויחו סכום כסף רב במסגרת ההימורים שביצעו, והמשיכו להמר גם על תקיפות ישראליות נוספות בהמשך השנה.

<u>שאלות לדיון:</u>

1. אילו ערכים נפגעו באירוע?
2. מה הפער המרכזי באירוע? מהן הסיבות לפער?
3. מהי האחריות שלנו באירועים מסוג זה?
4. כיצד ניתן למנוע אירועים מסוג זה בעתיד?

<u>דגשים למפקד:</u>

1. חידוד האחריות האישית שחלה על כל חייל ומפקד בצבא בעת חשיפה למידע צבאי בכלל ומידע מסווג בפרט.
2. שיתוף, העברה, מסירה והרחבת חשיפה למידע צבאי לגורם שאינו מורשה (בין אם הוא גורם צבאי / אזרחי) – הינה עבירה פלילית!
3. חשיבותו של עקרון המידור – בעלי תפקידים ייחשפו למידע הנחוץ לביצוע תפקידם, התואם את רמת הסיווג שלהם ובאישור גורם מוסמך.
4. עיבוד, התנהלות ושיח על מידע מסווג יבוצעו רק בפלטפורמות מסווגות ובסביבת עבודה צבאית.
5. אנשי מילואים – תרבות ביטחונית ומודעות נמוכה יותר, יש אחריות ובקרה פיקודית נמוכה יותר על אוכלוסייה זו.
6. נושאים צבאיים שיש להם השפעה על המימד האזרחי ו/או העורף – בעלי השפעה רגשית רחבה לכולם (משפחה, איום, חופשות, פגיעה באורח החיים הרציף), ומעודדים את יצר החטטנות, סקרנות ואף הרצון לשיתוף מידע צבאי לגורמים מחוץ לצבא.

אירוע 2- הוצאת מידע בסיווג 'סודי ביותר לשו"ס' חשיפתו ברכבת ישראל

תקציר האירוע:

קצינה בשירות קבע באגף התקשוב הוציאה מסמכים מסווגים בסיווג 'סודי ביותר לשו"ס', בהם היא עיינה וקראה במהלך נסיעתה ברכבת, כאשר תוכן המסמכים היה חשוף לעיניי אזרחים וגורמים רבים לא מורשים.
החומרים הוצאו משטח הבסיס הצבאי בצורה מודעת על ידי הקצינה, והאירוע התגלה מדיווח שהתקבל על ידי אחד מעוברי האורח.

שאלות לדיון:

1. אילו ערכים נפגעו באירוע?
2. מהי האחריות שלנו באירועים מסוג זה?
3. מה והאם יש הבדל בין חייל שלא פועל על פי הנהלים לבין חייל שעושה עבירת ב"ם מודעת ויזומה?
4. כיצד ניתן למנוע אירועים מסוג זה בעתיד?

דגשים למפקד:

1. רשלנות וביצוע עבירה בצורה מודעת ויזומה להוצאת מידע מסווג מחוץ לבסיס צבאי.
2. תפקידים אינטנסיביים, לחץ וריבוי משימות ואף מוטיבציית יתר – לעיתים עלולים להוביל לשיקול דעת שגוי ולקבלת החלטות שחורגת מפקודות והנחיות. במקרה הנ"ל הקצינה סיכנה סודות צבאיים ומידע מסווג.
3. חשיפה של מידע מסווג במקום ציבורי – מאתגר לבצע הערכת נזק ואומדן להתפשטות המידע מפאת העובדה שהוא נחשף בציבור והיה גלוי לאזרחים רבים, שלא ניתן לזהות/למנות אותם ואף לא להצביע על הרקע ממנו הם מגיעים.
4. הוצאת מסמכים מתוך בסיס צבאי היה יכול להוביל לאובדן המסמכים.

אירוע 3- כניסת טכנאי לחדר תקשורת וחיבור התקן חיצוני זר

תקציר האירוע:

באחד מבסיסי הפיקודים, בוצעו מספר פרויקטים הקשורים בבינוי, שיפוץ והסדרת תשתיות בבסיס.
במסגרת עבודות הקבלן שנעשו, הגיעו מספר רב של קבלנים לבסיס מידי יום.
סיווגם והרקע של הקבלנים נבדק בצורה חלקית, ואף בחלק מן המקרים הקבלנים נכנסו לשטח הבסיס ללא ליווי מתאים. יודגש כי עבודות הבינוי נעשו בתוך משרדים מתחמים מסווגים.
באחד מן הימים, עלה במסגרת ניטור שמבוצע ברשת חיבור של התקן חיצוני זר למחשב צבאי.
כחלק מתחקור ומיצוי האירוע, בדקו את מצלמות האבטחה ונמצא כי אחד מהקבלנים שמועסקים בפרויקט הבינוי, הסתובב ללא ליווי בשטח הבסיס, וכי הוא נכנס לחדר התקשורת (חדר שרתים מסווג) ואף חיבר למחשב צבאי התקן DOK.
מבדיקה לאחר מכן על הרקע של הקבלן, נמצא גם כי לקבלן לא היה סיווג מתאים. הקבלן הפסיק את עבודתו בפרויקט והועבר לחקירה בציר אזרחי.

שאלות לדיון:

1. אילו ערכים נפגעו באירוע?
2. מה הפער המרכזי באירוע? מהן הסיבות לפער?
3. מהי האחריות שלנו באירועים מסוג זה?
4. כיצד ניתן למנוע אירועים מסוג זה בעתיד?

דגשים למפקד:

1. צה"ל משתמש רבות במיקור חוץ ובאזרחים נותני שירות – שק"ם, טכנאים, שירות נקיון ואחזקה. בתוך כך, ישנה פקודה המחייבת בסיווג מינימלי (6 – שמור פיזי) לקבלנים ואזרחים נותני שירות לטובת כניסה לבסיס צבאי, וכניסתם צריכה להיות בבקרה ובליווי של גורם צבאי.
2. האחריות למימוש ההנחיה ובקרתה היא בראש ובראשונה של המפקד האחראי על הפרויקט.
3. קבלן הוא גורם זר שעצם כניסתו לתוך בסיס צבאי מקנה לו פוטנציאל וקרבה לליבת הסוד, נדרש להתייחס לכך בחומרה וברגישות המתאימה, להקפיד על ליווי מתאים ואף לגלות עירנות לגורמים שמסתובבים בשטח צבאי.
4. למניעת מקרים של חיבור התקנים חיצוניים למחשבים צבאיים ישנו רכיב פיזי שמונע מביצוע החיבור בפועל ('חסמב"ם'); אם הוא היה מותקן על גבי המחשב ייתכן וכי האירוע היה נמנע.

אירוע 4- העברת מידע התרעתי מסווג בטלפון הנייד

תקציר האירוע:

במהלך מבצע 'עם כלביא', סמב"צית מפיקוד העורף העבירה מידע מסווג אותו קיבלה לידיה במסגרת איוש משמרת בחמ"ל (תא דיווח).

המידע הועבר ע"י החמ"ל המרכזי, בו יושבים בעלי תפקידים בדרג גבוה וקבה"ח וגורמי מודיעין אל החמ"ל אותו היא איישה. המידע היה המבוסס על מידע מודיעיני המעיד על אינדיקציה והיערכות גורמי אויב למימוש ירי קינטי אל עבר שטח ישראל.

המידע הועבר לתא הדיווח לצורך היערכות מבצעית של החמ"ל והיחידה וכחלק מפו"ש דיווח סדור שמוגדר בעבודה השוטפת. הסמב"צית העבירה את המידע באמצעות אפליקציית 'WhatsApp' להוריה, בן זוגה ומעגל החברים – סה"כ הועבר לכ-30 אנשים שונים, ובו 4 תפוצות שונות.

המידע שהחיילת העבירה כלל מיקום, עיתוי ושעות מדויקות לירי והגורם שעתיד לממשו. לאחר שההודעה נשלחה ונקראה על ידי כל הנמענים, היא מחקה את הודעותיה ושלחה באותן תפוצות הודעה נוספת שניסוחה "לא שמעתם את זה ממני".

באחת הקבוצות שההודעה נשלחה אליה, אחד מחברי הקבוצה הגיב לחיילת שזו הינה עבירת ב"ם ושתמחק את הודעתה. בהתאם, החיילת מחקה את הודעותיה מאותה קבוצה, אך לא משאר הקבוצות והתפוצות בהן ההודעות הופצו. במסגרת פעילות ניטור של יחב"ם פיקוד העורף, האירוע נוטר וזוהה. החיילת תוחקרה וכך גם האירוע בציר מפקדים, בוצעו צעדים לצמצום הנזק ומיצוי לאירוע עצמו.

ברקע לאירוע:

- החיילת הייתה חדשה בתפקידה, הגיעה לפיקוד מרכז בסמוך לסיום הכשרתה כסמב"צית, ומועד התרחשות האירוע היה בסמוך לסיום הקורס שלה (וגיוסה לצה"ל). בנוסף, החיילת לא עברה תדריך ביטחון מידע פרונטלי, אלא דיגיטלי בלבד.
- החיילת ביצעה תחקיר ביטחוני לטובת ביצוע תפקידה בחמ"ל (לא נדרשה לסיווג קודם לכן, והחלה את תהליך הסיווג רק לאחר שיבוצה בפיקוד העורף). מפקדיה של החיילת אישרו להכניס את החיילת לחמ"ל, לבצע חפיפה ומשמרות על אף שסיווגה טרם אושר.

משמע, החיילת נכנסה לחמ"ל לצורך ביצוע תפקידה באישור מפקדיה כאשר יש לה סיווג לרמה 5 בלבד ('שמור').

שאלות לדיון:

1. אילו ערכים נפגעו באירוע?
2. מה הפער המרכזי באירוע? מהן הסיבות לפער?
3. מהי האחריות שלנו באירועים מסוג זה?
4. כיצד ניתן למנוע אירועים מסוג זה בעתיד?

דגשים למפקד:

1. תדרוך, הסברה, והמחשת החשיבות לנהלי ביטחון מידע קריטית להתנהלות תקינה של הארגון, בטח בקרב חיילים חדשים בצבא ו/או אוכלוסיות חדשות ביחידה.
2. אי ידיעת החוק אינה פוטרת מהעונש – ולכן נדרש גם מהפרט לדעת את הנהלים המחייבים בהתנהלות עם מידע צבאי.
3. נדרשת הקפדה יתרה על מידור מידע בין חמ"לים, ועל אופן העברת מידע והשימוש שנעשה בו. גם כאשר מידע מועבר בין חמ"לים לפי ציר דיווח סדור, ישנה אחריות למעביר המידע לחדד את אופן ההתנהלות עם אותו מידע ולוודא שהמידע עובר לאדם שאכן רשאי להיחשף אליו.
4. סיווג ביטחוני הינו הכשר לביצוע תפקיד מסווג וחשיפה למידע רגיש, ואין בסמכות מפקד יכולת החרגה לתנאי זה.

אירוע 5- פרסום סרטון ברשת החושף שיטה מבצעית

תקציר האירוע:

במסגרת מספר פעילויות מבצעיות שבוצעו בחיל האוויר, פורסם באפליקציית Facebook סרטון ותמונות של מספר חיילים בתפקידי תמיכה טכנית ותחזוקה, בו רואים בבירור את החיילים במהלך תחזוקת כלי טיס המשמש לפעילות חשאית מסווגת.

הסרטון שעלה לרשת לא פורסם ע"י מקור רשמי (כתב/דובר צה"ל), וצולם בתוך מבנה של אחת מטייסות חה"א.

במסגרת הסרטון ולמספר בודד של שניות, מבחינים במכשיר קשר (מסווג), שייחודי לפעילות המסווגת שבוצעה ולמתאר החשאי שמאפשר שמירה על חשאיות והקטנת החתימה בשטח.

באותה תקופה, בוצעו בתדירות גבוהה פעולות במתאר הזה לתכליות מבצעיות, והנ"ל היה סמוך לאחת מהמערכות של צה"ל אל מול איראן.

פרסום הסרטון ברשת הגלויה הגיע לידי חוקר שמוצאו באחת ממדינות האויב, ובאמצעות תצלום בלבד זה המכשיר הוא הצליח להגיע לניתוח ופירוט טכני מתקדם ומעמיק אודולת המכשיר ופעולתו.

בתוך הניתוח שהוא ביצע, הוא הצליח לחשוף את אותה שיטת פעולה ייחודית שמקנה חשאיות.

שאלות לדיון:

1. אילו ערכים נפגעו באירוע?
2. מה הפער המרכזי באירוע? מהן הסיבות לפער?
3. איך ניתן לחזק גאווה יחידתית בלי לעבור על הנחיות ופקודות ביטחון מידע?
4. כיצד ניתן למנוע אירועים מסוג זה בעתיד?

דגשים למפקד:

1. משמעת רפויה על הנחיות ביטחון מידע – צילום בתוך מתחם מסווג, של טכנולוגיו וכלי טיס, ואף צילום של החיילים עצמם שחלקם שוהים תחת פקודת 'נהלי חשיפה' שלא מאפשרת חשיפה שלהם בפנים גלויות ו/או שיוך כלל לצה"ל.
2. הבנה חלקית של הנחיות ומשמעות ביטחון המידע והסכנה שיש בסושיאל וברשתות החברתיות – המידע מגיע בצורה מיידית, מופץ בתפוצה רחבה וגלובלית, וכל פרסום/תיעוד, גם כזה שנראה הכי 'תמים', יכול להביא לפגיעה מבצעית חמורה.
3. בתקופות בעלות עומס מבצעי, נכון לחדד הנחיות מחייבות/עקרונות חשובים בעבודה, ביניהם גם ביטחון מידע לצמצום הפוטנציאל להתממשות של תקלות ב"ם.

אירוע 6- דלף מידע מבצעי שנוצר מתשתית אויב ברשת החברתית ופנייה למשרתי צה"ל

<u>תקציר האירוע:</u>

במהלך מלחמת 'התקומה' זוהו מספר אינדיקציות שמצביעות על נגישות גורמי מ"ן אויב למספר בסיסים ומתקני צה"ל, המקנה להם תמונת חשיפה מלאה על שגרת הפעילות המבצעית באותם בסיסים, סדרי כוחות, מיקוד מבצעי.

בנוסף, במסגרת הנגישות גורמי מודיעין האויב הצליחו להעלות מספר פעמים התרעות מקדימות לפני פעילות צבאית, מה שגרם להיערכות מקדימה של צד אדום וצמצום חופש הפעולה ואפקט ההשפעה על פעילות צה"ל.

ממחקר שבוצע על אופן השגת הנגישות, נמצא כי הנגישות והתשתית מתבססת על רשתות חברתיות – במסגרתה הוקמו מספר רב של ישויות המזדהות כנשים (כשבפועל הפרופיל הרשתי מתוחזק ומנוהל ע"י גורם מודיעין זר).

אותן "נשים" יצרו קשר וביססו שיח עמוק שרובו בעל אופי רומנטי עם אזרחים ומשרתי צה"ל בסדיר ובמילואים.

הפרופילים שהוקמו ברשת היו בעלי חזות המייצרת אמינות – תמונות, מידע וויזואליה רבים, מספר לא מבוטל של חברויות וקשרים ברשתות החברתיות והתדמית החיצונית של כל פרופיל תוכננה באופן שמציג כל בחורה כנאה ו"אמיתית", וביסוס האמינות המשיך גם במסגרת השיחות והקשר הפרטני שהישות הפיקטיבית יצרה עם כל אזרח/משרת – התנסחות בעברית ברמה טובה, שימוש בביטויים שמוכרים בשפה העברית ה"יום-יומית"/חברה ישראלית ובניב ומונחים שיהיו בשימוש בשיח שוטף על ידי מי שדובר את השפה העברית כשפת אם/שפה ראשית.

הפרופילים עבדו כקבוצה ובאופן שיטתי – פנייה מסיבית למספר רב של משרתי צה"ל בכל יום, שמירה על שיח וקשר רציף לצורך ביסוס אמון וקשר אישי עם כל אדם, תכנון וחלוקה מראש של הפניות בין הישויות כך שלא תהייה כפילות בפנייה של מספר פרופילים לאותו אדם (זאת לצורך ניצול מיטבי של תשתית העבודה).

בנוסף, בוצעו התאמות בסוג הפרופיל ("בחורה") שתפנה לכל אדם, צורת ההתנסחות ושיח שהיו מותאמים לאוכלוסיות המפולחות לפי גילאים, מגדר, תפקידים, מצב משפחתי (רווק/נשוי/גרוש וכו'), דרג בצבא וכו'.

אופי פעולה מתוחכם ומנוהל כפי שתואר קודם, איפשר לתשתית הזו לעבודה בצורה מקיפה ואפקטיבית, ביסס קשרי אמון אישיים ועמוקים בין ישויות פיקטיביות למשרתי צה"ל בסדיר ובמילואים שלבסוף הביאו לתרומות מודיעיניות משמעותיות לגורמי מודיעין האויב, פגיעה בפעילויות צבאיות מבצעיות, חשיפת נקודות תורפה של צה"ל, פגיעה בחשאיות ואפקט ההפתעה.

תרומה משמעותית כזו נגרמה על ידי רשלנות של מספר רב של משרתי צבא בחובה/קבע/מילואים ולא רק בדרג זוטר.

כחלק ממנגנון הטיפול באירוע, סוכלו חלק מן הישויות, ומשרתי צה"ל שאליהם התקבלו פניות ו/או כאלו שביססו קשר עם הפרופיל הזדוני נלקחו לחקירה הן להערכת נזק והן לחשיפה על הזהות האמיתית של הישויות והתשתית הכוללת ותודרכו בהתאם.

יצוין כי בחלק מן המקרים, גם לאחר חשיפת האמת על זהות הפרופילים, היו מספר של משרתי צה"ל שחזרו לנהל ולתחזק את הקשר הרומנטי עם אותן דמויות ברשת, והדבר נובע גם מלחץ ופניות חוזרות מאותם פרופילים וגם מאמון עמוק ורגש/תלות שאותו משרת פיתח לישות ברשת.

מקרים אלו טופלו, אך הם מעידים על מידת העומק, הקשר והאמינות שכל אחד מן הפרופילים הצליח ליצור מול משרתי צה"ל אליהם הן פנו.

שאלות לדיון:

1. אילו ערכים נפגעו באירוע?
2. מה הפער המרכזי באירוע? מהן הסיבות לפער?
3. איך ניתן להסביר את התופעה שחיילים חזרו לדבר עם הפרופיל גם אחריו שהובהרה זהותו?
4. כיצד ניתן למנוע אירועים מסוג זה בעתיד?

דגשים למפקד:

העברת מידע צבאי בעל רגישות, ערכיות וסיווג רב לאורך תקופה ארוכה ובמהלך מלחמה עצימה שצה"ל מצוי בה מעידה על התנהלות ומודעות ביטחונית נמוכה של אותם משרתים – החל מחוסר מודעות לאיומים במרחב הרשת, הפרה בוטה של נהלי ביטחון מידע בדבר שימוש, עיבוד ואחסון מידע צבאי והעברתו לגורם לא מורשה (גם אם לא היה מדובר בפרופיל ששייך לתשתית אויב, אלא אזרח ואדם פרטי).

העברה של מידע צבאי מסווג בתשתית אינטרנטית ואף מסירתו לגורם וירטואלי יכולה להעיד על שיקול דעת/חוסר הבנה לסכנה שבהעברת המידע והעלאתו לרשת ואף בחלק מן המקרים יכולה להעיד על כוונת זדון ושימוש לרעה במידע.

בנוסף, נשקף חוסר הבנה לאיום ולסיכון שישנו ברשת החברתית – אין לדעת מי נמצא מאחורי המקלדת, אין מספיק חשדנות לפניות שמתקבלות ברשת ולגורם שאליו מעבירים מידע מכל סוג – אישי, פרטי, צבאי וכו'.

אירוע 7-המתחזה מפד"ם

<u>תקציר האירוע:</u>

בחודש אוקטובר 2023, מספר ימים מפרוץהמלחמה, התגלה בפיקוד דרום אזרח אשר התחזה לקצין במילואים בדרגת סרן, שהזדהה כקצין שאחראי על מבצעים מיוחדים.

האזרח נכנס בתאריך 08/10/2025 לבסיס פיקוד הדרום בפעם הראשונה (נכנס תוך שהוא קופץ מעל שער הכניסה), ביצע פגישות עם מספר מפקדים ובע"ת בכירים בסדיר ומילואים בפיקוד, תוך שהוא מציג את עצמו קצין מבצעים מיחידה מסווגת, והמשיך להגיע ליחידה ברצף מספר ימים לאחר מכן.

במסגרת שהותו בבסיס, המשיך להפגש עם מפקדים ובעלי תפקידים בתחומים השונים בדרגים ליבתיים (סא"ל ומעלה), נכנס לדיונים מסווגים רבים, הצליח לייצר כתב מינוי רשמי וחתום ע"י קצין בכיר בדרגת אל"ם אותו הכיר משירותו הצבאי הסדיר, מה שבהמשך הדרך גם הקנה לו אישור כניסה לבסיס.

בסמכותו של כתב המינוי נפתח תא מיוחדים בחמ"ל המרכזי, עליו הקצין המתחזה פיקד, והוקצו לו חיילים ומשאבים תואמים לצורך ביצוע משימתו.

בהמשך פעולותיו, הקצין הגיע גם לבסיס הקריה, נפגש עם מספר בעלי תפקידים שהבכיר מהם היה בדרגת תא"ל, בנושא מבצעים מיוחדים המתוכננים במסגרת המלחמה.

עוד הצליח להיכנס בצורה עיתית להערכות המצב, ואף לביקורו של שר הביטחון בחמ"ל פיקוד הדרום.

האזרח תיעד את כל פעולותיו, המידע שקיבל ונמסר אליו / נחשף אליו במסגרת דיונים וכל מידע אחר במחברות, לטפופים, ושימוש במכשירי הסרטה והקלטה ומספר מכשירים ניידים.

האזרח בשירותו הסדיר היה קצין ביחידת מגלן, והשתחרר בדרגת סגן לאחר כ5 שנים בשנת 2018.

הוא הזדהה במספר שמות ובדרגות שונות (רס"ן/סרן) ואף התאים ודייק את תפקידו בהתאם לבעל התפקיד איתו הוא שוחח.

הקצין שהתחזה הצליח לייצר יחסי אמון, ביסוס לתפקידו ותכליתו המבצעית בפני בעלי התפקידים השונים שאיתם הוא נפגש, הצליח לייצר קשרי עבודה בסיסיים עם בעלי תפקידים רבים בתפקידי מפתח ו/או בדרגות בכירות וכל זאת בטווח זמן קצר.

בתאריך 15 באוקטובר 2023, 8 ימים לאחר פעילותו וכניסתו הראשונה בזהותו הבדויה, נתפס הקצין על ידי השב"כ, הודות לדיווח ע"י קצין מאמ"ן שהועבר לגורמי ביטחון מידע בפיקוד דרורם הקשור באירוע חריג בו האזרח המתחזה היה מעורב.

מבדיקה שנעשתה בציר ביטחון מידע, התגלה האירוע וזהותו האמיתית של האדם.

שאלות לדיון:

1. אילו ערכים נפגעו באירוע?
2. מה הפער המרכזי באירוע? מהן הסיבות לפער?
3. איך שומרים על משמעת ב"ם ועמידה בפקודות כשהיחידה נמצאת בחירום, בעומס, שחיקה וגיוס רחב של אנשי מילואים?
4. כיצד ניתן למנוע אירועים מסוג זה בעתיד?

דגשים למפקד:

1. האיום הפנימי יכול להתממש בכל מקום, בכל תקופה ועל ידי כל אדם – בין אדם האדם נמצא בשירות פעיל, בתקופת מלחמה וזהו איום שמאתגר לעיתים לזהותו בשטח.
2. בעיתות וקצבים מבצעיים גבוהים ואף באירועים בהם מזמנים כמות רבה של אנשי מילואים - לעיתים מאתגר לשלוט בכל כוח האדם, החל מזיהוי ראשוני, בקרה, שיח וכו'.
3. האזרח המתחזה הצליח לאסוף ולהשיג נגישות למידע צבאי רב, להיכנס לדיונים ומתחמים רבים ולהתברג במהירות בשגרת העבודה המבצעית בפיקוד, וגורם משמעותי שתרם לכך היה אדישות וחוסר עירנות ופער בדיווח של שאר המשרתים ביחידה לזיהוי ותשאול האדם, קיום פגישות, שיתוף פעולה ומסירת מידע ב'קלות דעת' ללא ווידוא זהות ותפקידו האמיתי של האדם.
4. בחקירת האירוע ובדיוני בהימ"ש, האזרח הואשם בריגול ללא כוונה לפגיעה בביטחון המדינה – אמנם לא נמצאה כוונת זדון / קשר לגורם מודיעין זר, אך מצבי חירום לצד ערכים, נורמות ומוטיבציות שמשתנות בין אדם לאדם יכולות להוביל אותו לפעול בצורה שמנוגדת לחוקים, ולבצע דברים קיצוניים שאף אסורים מבחינה חוקית.
5. האירוע מלמד על פערי אבטחה – כניסתו הראשונה לבסיס התבצעה מקפיצה מעל שער הכניסה.
6. פער במידור ליבות סוד – כניסתו לחמ"לים ומכלולים רבים, ללא התערבות/בקרה/זיהוי על ידי בעל תפקיד או אחד מהמפקדים במכלול.

אירוע 8-הפצת גרף צה"ל לשנת 2026 בWhatsApp

תקציר האירוע:

במהלך חודש אוקטובר 2025, הופץ ברשת הצבאית ע"י חטיבת המבצעים מסמך במעמד טיוטא המפרט את גרף הלחימה של צה"ל לשנת 2026.

המסמך הופץ ברשת ה-ArmyTS, רשת בסיווג סודי ביותר לרשימת תפוצה בה נכללים בעלי תפקידים העוסקים בתכנון מבצעי, תע"ם, הכשרות ואימונים בפיקודים ובאגפים השונים בצבא כחלק מהעבודה השוטפת לסנכרון מבצעי.

אחרי ההפצה המטכ"לית של המסמך, הוא הועבר מדרג הפיקוד ליחידות, אוגדות וחטיבות בצה"ל.

יום למחרת, מתקבל דיווח לחטיבת המבצעים כי המסמך מופץ בתפוצה רחבה בקבוצות ותפוצות WhatsApp רבות.

הדיווח התקבל ע"י קצין ביטחון מידע מאחד הפיקודים, שנתקל בהודעה ובמסמך.

המסמך שהופץ ברשת הצבאית, הודפס ונסרק לטלפון הנייד והופץ בתצורה הזו בקבוצות צבאיות רבות; מעריכים כי הוא הופץ לכ-400 נמנעים/קבוצות בתווך האזרחי.

מבירור ותחקור של האירוע, נמצא כי כבר בהפצה ברשת הצבאית של המסמך הוא הופץ (לא על ידי המפיץ הרשמי) לעוד 30 תפוצות שקיימות בצ'אט המבצעי / HiChat, ול143 שיחות פרטיות מעבר לרשימת התפוצה שנקבעה על ידי מפיץ הרשומה.

התפוצות השונות שאליהן הגיע המסמך מונות משתמשים תפקידניים – משתמש ברשת שעליו עובדים מספר אנשים (לדומא יוזר חמ"ל).

בנוסף, במסגרת מאמצי ניטור זוהתה אינדיקציה גבוהה לכך שהמסמך הגיע לצ'אטים ותפוצות של ערוצים פלסטיניים ואיראנים.

שאלות לדיון:

- אילו ערכים נפגעו באירוע?
- מה הפער המרכזי באירוע? מהן הסיבות לפער?
- כיצד ניתן למנוע אירועים מסוג זה בעתיד?

דגשים למפקד:

1. גם למידערגיש שמופץ ברשת חשוב להקפיד על מנגנוני בקרה והגנה תואמים – חידוד איסור להעברת החומר למי שמקבל לידיו את המידע, הגדרת סיסמא למסמכים ואף הגדרה טכנית בהפצת המייל כי לא ניתן להעבירו/לשרשרו.
2. המידע הופץ בצורה ויראלית ורחבה במרחב האינטרנט ותשתית הWhatsApp, וייתכן כי בעוד פלטפורמות ויישומים נוספים. חלק עיקרי (ואם לא מירבי) שקיבלו לידם את המידע היו משרתי צה"ל, שלא ראו בהעברת המידע תקלה/אירוע חריג/סכנה לסוד, ויתרה מכך – גרמו להרחבה יזומה של המידע לגורמים ותפוצות נוספות בעצמם.
3. שיתוף המסמך והמידע בתוך הרשת הצבאית ואף מחוצה לה היה בצורה קלת דעת, ללא הבנה של הסכנה בהרחבת תפוצתו ושבירת מסגרות המידור. בנוסף, במרבית מן המקרים לא בוצע אימות לזהות או בעלי התפקידים שקיבלו את המידע – האם המידע אכן נדרש לצורך ביצוע תפקידם, האם יש להם סיווג מתאים והאם כותב ומפיץ הרשומה מאשר להעביר לאותו גורם את המידע, שכן הוא הגורם היחיד שמוסמך לכך לפי פ"מ אבטחת רשומות.