תבנית למסמך תחקור

שם חברה

תוכן נתונים

[פרטים במסמך 4](#_Toc126610443)

[עורכי המסמך 4](#_Toc126610444)

[גורם מאשר 4](#_Toc126610445)

[גרסת מסמך 4](#_Toc126610446)

[תקציר מנהלים 5](#_Toc126610447)

[פגיעה ומידת הנזק 6](#_Toc126610448)

[השפעות עסקיות 6](#_Toc126610449)

[תחקיר ופרטי האירוע 7](#_Toc126610450)

[דיווח התקרית/האירוע 7](#_Toc126610451)

[גורמים שעודכנו באירוע 7](#_Toc126610452)

[מאפיינים מרכזיים בתקרית/אירוע 7](#_Toc126610453)

[מהלך וטיפול בתקרית/אירוע 8](#_Toc126610454)

[פרטי בנסכים בתקרית/אירוע 9](#_Toc126610455)

[ניתוח התקרית/אירוע 10](#_Toc126610456)

[הקדמה טכנית 10](#_Toc126610457)

[תהליכי ופעולות תוקף 10](#_Toc126610458)

[סדר פעולות תקיפה 10](#_Toc126610459)

[גרף ראיות תקיפה 11](#_Toc126610460)

[תהליכי Kill Chain 11](#_Toc126610461)

[סיווג מבוסס MITRE ATT&CK 11](#_Toc126610462)

[ראיות וממצאים 11](#_Toc126610463)

[משפחות וסוגים 11](#_Toc126610464)

[כתובות תקיפה 11](#_Toc126610465)

[התנהגות תקיפה 11](#_Toc126610466)

[לוגים 11](#_Toc126610467)

[ניתוח האירוע 11](#_Toc126610468)

[כשלים בתקרית/אירוע 12](#_Toc126610469)

[מתווה פעולות 13](#_Toc126610470)

# פרטים כללים

## עורכי המסמך

|  |  |
| --- | --- |
| שם מלא | תפקיד |
|  |  |
|  |  |
|  |  |
|  |  |

## גורם מאשר

|  |  |
| --- | --- |
| שם מלא | תפקיד |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## גרסת מסמך

|  |  |  |
| --- | --- | --- |
| תאריך יצירה/עריכה | גרסת מסמך | הערות |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# תקציר מנהלים

מיועד לרובד הניהולי ולכן אין לכלול פירוט טכני אלא אזכור כללי בלבד.

תקציר מנהלים כללי עם נגיעות טכניות קלות בלבד. שכולל את הנקודות הבאות:

אבני דרך בתקרית / אירוע

תאריכים חשובים

תאריכי דיווח

צעדים שננקטו

מצב קיים

מצב עתידי

השפעות עסקיות

כלל הנקודות המוזכרות צריכות לקבל תיאור ופירוט

## פגיעה, פוטנציאל ומידת הנזק

|  |  |
| --- | --- |
| האם ישנה פגיעה בנכס חיצוני או פנימי של הארגון | כן  לא |
| הוצאת נתונים מתוך נכסים בארגון | כן  לא |
| האם היה העלאת נתונים לרשת ציבורית | כן  לא |
| האם היה פרסום נתונים במדיות השונות (דארקווב, טלגרם וכו) | כן  לא |
| האם ישנה פגיעה בתדמית הארגון | כן  לא |
| האם האירוע צריך להיות מתוקשר | כן  לא |
| האם ישנה מעורבות של המחלקה המשפטית באירוע | כן  לא |
| האם ישנה מעורבות של חטיבת GRC | כן  לא |
|  |  |

## השפעות עסקיות

|  |  |
| --- | --- |
| גורם מושפע (חטיבה/חברה/פרויקט) |  |
| האם ישנה השפעה עסקית ישירה | כן  לא |
| האם ישנה השפעה עסקית עקיפה | כן  לא |
| יש לפרט השפעות עסקיות כלשהן | |
| האם ישנו אישור של גורם עסקי | כן  לא |

# תחקיר ופרטי האירוע

## דיווח התקרית/האירוע

|  |  |
| --- | --- |
| גורם מדווח |  |
| תפקיד מדווח |  |
| תאריך דיווח למנהל/ת אבטחת מידע |  |
| תאריך דיווח לגורם עסקי |  |
| תאריך דיווח להנהלה |  |
| תאריך דיווח למחלקה המשפטית |  |
| תאריך דיווח למחלקת PR |  |
| תאריך דיווח לצוותים אחרים (יש לפרט) |  |

## גורמים שעודכנו באירוע

|  |  |
| --- | --- |
| שם מלא | תפקיד |
|  | מנהל/ת אבטחת מידע |
|  | CEO |
|  | CIO |
|  | מנהל/ת חטיבה |
|  | מנהל/ת מחלקה |
|  | מנהל/ת צוות |
|  |  |

## מאפיינים מרכזיים בתקרית/אירוע

|  |  |
| --- | --- |
| שם ומזהה האירוע |  |
| תאריך זיהוי ראשוני |  |
| תאריך דיווח ראשוני |  |
| תאריך דיווח למנהל/ת אבטחת מידע |  |
| אופן הדיווח |  |
| תאריך דיווח לגורם עסקי |  |
| מצריך דיווח להנהלה |  |
| אירוע חדש | כן  לא |
| אירוע חוזר | כן  לא |
| תאריך תגובה ראשוני לאירוע |  |
| גורם מגיב ראשוני לאירוע |  |
| האם בוצעה הערכת מצב והכרזה על אירוע | כן  לא |
| סוג תקרית/אירוע |  |
| כלי שזיהה את האירוע |  |
| האם מדובר על תקיפה מוכרת | כן  לא |
| שם קבוצת תקיפה | תיאור לקבוצות תקיפה  [Threat Actors (powered by MISP)](https://malpedia.caad.fkie.fraunhofer.de/actors) |
| טקטיקות והתנהגות נוספת באירוע |  |
| מטרת קבוצת התקיפה או הגורם התוקף |  |
| בוצעה בדיקה של פרצות/תקיפות נוספות האם |  |
| האם מדובר על אירוע משנה | כן  לא |
| במידה ויש אירוע מקביל או משנה, יש לפרט |  |
| האם יש לתוקפים דרישות | כן  לא |
| מטרות ודרישות התוקפים |  |
| יש לפרט לגבי נתונים שדלפו |  |
| האם נפגעו שירותים/תהליכים? נא לפרט לפי הצורך בסימון. | כן  לא |
| האם היה פרסום בערוצים השונים | כן  לא |
| כלים באירוע |  |

## מהלך וטיפול בתקרית/אירוע

|  |  |
| --- | --- |
| תגובה ראשונית באירוע |  |
| גורם ראשוני שהגיב לאירוע |  |
| משך זמן האירוע |  |
| תאריך הכלה ראשוני |  |
| סוג הכלה |  |
| גורמים שטיפלו באירוע |  |
| יש לפרט מנהל האירוע ואנשי מפתח |  |
| האם מנהל/ת אבטחת מידע עודכנ/ה באופן רציף | כן  לא |
| האם האירוע נוהל מתוך חדר מצב באופן רשמי | כן  לא |
| האם בוצעו פגישות סטטוס בפרקי זמן מוגדרים מראש | כן  לא |
| האם היה תקשורת רציפה בין הצוותים הפועלים באירוע | כן  לא |
| האם הוקם ערוץ תקשורת לאירוע | כן  לא |
| האם שותפו ראיות וממצאים באופן רציף בין גומרי התחקור | כן  לא |
| האם היה מעורבות תחקור של גורם חיצוני | כן  לא |
| האם היה תיעוד של תהליכים, ראיות והערות במהלך התקרית/אירוע? | כן  לא |
| מהם הכלים שהיו בשימוש בתקרית/אירוע |  |
|  |  |
|  |  |

## פרטי נכסים בתקרית/אירוע

|  |  |
| --- | --- |
| שם הנכס |  |
| תפקיד הנכס |  |
| סביבת הנכס |  |
| נכס מבצעי |  |
| האם מדובר בנכס חיוני/רגיש/ליבה | כן  לא |
| האם מקושר לאפליקציות בתוך הארגון | כן  לא |
| מקושר לאפליקציות מחוץ הארגון (כולל צד שלישי) |  |
| ישנו מיפוי ותרשים כל הנכס וסביבתו | כן  לא |
| רישום הנכסים |  |
|  |  |
|  |  |
|  |  |

# ניתוח תקרית/אירוע

## הקדמה טכנית

## תהליכי ופעולות תוקף

## סדר פעולות תקיפה

## גרף ראיות תקיפה

## תהליכי Kill Chain

## סיווג מבוסס MITRE ATT&CK

# ראיות וממצאים

## משפחות וסוגים

## כתובות תקיפה

## התנהגות תקיפה

## לוגים

## ראיות נוספות

## ניתוח נוסף

# כשלים בתקרית/אירוע

# מתווה פעולות