

**סקר אבטחת**

**מידע**

**מערכת Bookstack**

פברואר

2025

[1. תקציר מנהלים 3](#_heading=h.gjdgxs)

[הקדמה 3](#_heading=h.30j0zll)

[תיחום הסקר 3](#_heading=h.1fob9te)

[תרחיש ייחוס 4](#_heading=h.3znysh7)

[רמת הסיכון 4](#_heading=h.2et92p0)

[2. מיפוי נכסי מידע ומאגרי מידע 5](#_heading=h.tyjcwt)

[3. מיפוי תהליכים טכנולוגיים 6](#_heading=h.3dy6vkm)

[4. סיכונים מרכזיים שזוהו 7](#_heading=h.1t3h5sf)

# 1. תקציר מנהלים

## 

## הקדמה

סיכוני סייבר מהווים חלק משמעותי מכלל הסיכונים התפעוליים אליהם

חשופות חברות ולהתממשותם עלולות להיות השלכות עסקיות שונות, לרבות:

פגיעה במוניטין, אובדן הכנסות, חשיפה משפטית וכו.'

מטרות העל של תהליך ניהול סיכוני סייבר הן הפחתת הסבירות לפגיעה בתהליכים העסקיים ובמידע של הארגון כתוצאה מהתממשות סיכונים אשר מקורם במרחב הסייבר, וצמצום ההשפעה עליהם, במקרה שהתממשו סיכונים אלו.

כדי להפחית סיכוני סייבר באופן שיטתי, יעיל ואפקטיבי, נדרש למפות נכסי מידע ותהליכים עסקיים, ולזהות את סיכוני הסייבר אליהם הם חשופים. לאחר מכן יש לגבש תוכנית הפחתה, תוך תיעדוף הטיפול בסיכונים, בהתאם לעוצמתם ולמידת השפעתם על השגת יעדי החברה. גישה זו תסייע גם בתהליך קבלת ההחלטות באשר למשאבים אותם נדרשת החברה להשקיע בהגנת סייבר.

תהליך ביצוע סקר סיכוני סייבר מאפשר:

* לזהות את סיכוני הסייבר העלולים לפגוע בהשגת היעדים העסקיים.
* להעריך את רמת הסיכון תוך שקלול מרכיבי עוצמה וסבירות.
* להעריך את אפקטיביות סביבת הבקרה של מערכות המידע התומכות

בתהליכים עסקיים.

* להציג בפני הנהלה ודירקטוריון תמונת מצב עדכנית לשם קבלת החלטות.

על מנת לקבל תמונת מצב עדכנית של מרחב הסייבר ומשטח התקיפה אליו חשופה החברה , נתייחס להיבטים הבאים:

* תיאור התהליך העסקי מקצה לקצה
* מיפוי נכסי מידע ומאגרי מידע של החברה
* סיכוני סייבר נפוצים בהתאם למערכות החברה

## תיחום הסקר

במסגרת הסקר נבדקו בין היתר הנכסים והתהליכים הבאים:

* מערכות התקשוב של החברה
* גישה לסביבות הליבה בדגש על סביבת הפיתוח
* ניהול קוד
* ניהול גיבויים ותצורת שינויים

## תרחיש ייחוס

תרחיש הייחוס נגזר מאופי החברה ומתחומי פעילותה והוא מהווה בסיס לתהליך הערכת הסיכונים ולקביעת היקף ומטרות תוכנית הפחתת הסיכונים. בעת גיבוש התרחיש, יש לשקול מיהם השחקנים שעלולים לפעול כנגד החברה, מהי המוטיבציה לפעילותם, מטרות התקיפה והשלכותיה.

מניתוח אופי החברה ותחומי פעילותה, אשר התבצע עם תחילת סקר הסיכונים,

גובש תרחיש הייחוס המתואר להלן:

תוקף חיצוני המבקש להשיג רווח כספי / יתרון תחרותי או לשבש מידע ולגרום לנזק תדמיתי באמצעות גישה בלתי מורשית לאתר האינטרנט או/ו לשרתי הפיתוח או/ו למסדי הנתונים של החברה לשם גניבת פרטים אישיים או נתונים עסקיים אודות ספקים ולקוחות.

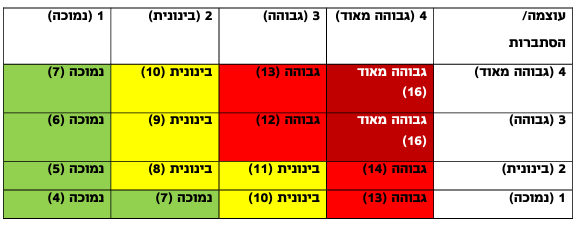
לחילופין, גורם פנימי, בדגש על עובד ממורמר, המבקש לנקום בחברה או להשיג רווח כספי עלול לנצל את הגישה שלו למערכות המידע לשם שיבוש תהליכים עסקיים או ביצוע הונאה.

## 

## רמת הסיכון

רמת הסיכון המרבית שזוהתה בחברה היא גבוהה.

רמת הסיכון חושבה ע"י הצלבת ערכי הסבירות ועוצמת הסיכון לפי המטריצה הבאה (מבוססת על תוה"ג של מערך הסייבר הלאומי):



# 2. מיפוי נכסי מידע ומאגרי מידע

להלן מיפוי נכסי המידע בארגון שתועדו במהלך הסקר:

| נכס | סוג הנכס | תצורת פריסה | ייעוד הנכס | רגישות המידע |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 3. מיפוי תהליכים טכנולוגיים

להלן מיפוי התהליכים הטכנולוגיים המנוהלים בחברה שתועדו במהלך הסקר:

| תיאור תהליך | גורם אחראי | פירוט |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 4. סיכונים מרכזיים שזוהו

להלן פילוח סיכוני הסייבר שזוהו במסגרת סקר הסיכונים בהתאם לרמת החומרה שלהם:

הסיכונים אשר זוהו במהלך הסקר הם כדלקמן:

| תיאור הסיכון | תרחיש | השלכות | רמת חומרת הסיכון | המלצות |
| --- | --- | --- | --- | --- |
| 1. דלף מידע רגיש מאתר האינטרנט הראשי של החברה | תוקף המנצל חולשות באבטחת אתר האינטרנט לשם גישה בלתי מורשית  לנתונים השמורים בו, דוגמת לקוחות , מידע עסקי (מילון) , וכו' | חשיפת נתוני לקוחות או כל מידע רגיש אחר השמור באתר האינטרנט עלולה  להוביל לנזק מהותי למוניטין החברה, ולנזק פיננסי בעקבותיו. | גבוהה | * מומלץ כי תיושם מתודולוגיית פיתוח מאובטח באתר האינטרנט. * מומלץ לבצע סקרי סיכונים וreview- code טרם העברה לייצור של פיתוחים   ושינויי תוכנה.   * מומלץ לקיים מבדקי חדירה עיתיים לאתר האינטרנט. * מומלץ לקבל התרעות אודות חולשות בספריות צד ג' בהן נעשה שימוש בקוד |
| 2. שיבושים בפעילות אתר האינטרנט הראשי של החברה | תוקף היוצר עומס על משאבי האתר, למשל באמצעות שימוש ברשתות מחשוב  שבשליטתו (Botnets) היוצרות היקף חריג של פניות לאתר, או, לחילופין,  השחתת האתר באופן המונע אפשרות של שימוש | אי זמינות אתר האינטרנט של החברה יוביל לפגיעה ביכולת לספק שירות ללקוחותיה ולפגיעה בהיקף המכירות. יתרה מכך, השחתת אתר אינטרנט מתפרסמת בתוך פרק זמן קצר יחסית בכלי התקשורת ופוגעת במוניטין החברה | גבוהה | * מומלץ לשקול הטמעת כלי אבטחה וניטור רלוונטיים לאתר האינטרנט, דוגמת   .Web Application Firewall   * מומלץ לשקול הטמעת מנגנון להתמודדות עם מתקפות מניעת שירות מבוזרות. * מומלץ לנטר באופן שוטף את אתר האינטרנט, לרבות בהיבט היקף תעבורה   שוטפת, ריבוי ניסיונות גישה כושלים וכו'   * יש להפריד סביבות DEV/TEST/PROD לחשבונות AWS שונים |
| 3. פגיעה בשרידות האתר ושירותי המערכת של החברה | בעיית שרידות של שרתי הפיתוח בעקבות תקלה בלתי צפויה. או לחלופין בשל עבודת תחזוקה יזומה (דוגמת התקנת עדכוני אבטחה המחייבים אתחול השרת) או תחזוקה יזומה מצד ספק הענן, דוגמת עדכון firmware | אי זמינות אתר האינטרנט של החברה יוביל לפגיעה ביכולת לספק שירות ללקוחותיה ולפגיעה בהיקף המכירות | גבוהה | * יש להקים לפחות שני שרתים נפרדים, כל אחד ב-Availability zone נפרד, באותו אזור גיאוגרפי (Region) ולחשוב על פתרון גישה שריד עבור השירות, החל מהפניית תעבורת תקשורת על-בסיס פניה לשירות DNS (בתצורת Round Robin) ועד מיקום השרתים מאחורי שירות Load Balancer אשר יידע לנתב את התעבורה בין השרתים, לבדוק Health של כל אחד מהשרתים לפני הפניית תעבורה וכו'. * על-מנת ליישם שרידות לשירותים, כדאי לבחור בפתרונות Load Balance מנוהלים. דוגמת Amazon ELB * מכיוון שמדובר בשירותים מנוהלים, ספק הענן דואג ל-scale (בהתאם לעומסים) ולשרידות הפתרון (חלוקה על פני מספר Availability zones). * לגבי פתרונות מנוהלים ל-Relational databases   חשוב להבין כי אומנם מדובר בפתרון מנוהל הכולל בתוכו עדכוני אבטחה וגיבויים, אך כברירת מחדל הטמעת instance בודד אינה מהווה פתרון שריד. |
| 4.גניבת מידע רגיש כגון סיסמאות , API keys ופרטי הזדהות נוספים ממחשבי המפתחים | תוקף אשר קיבל גישה לאחד ממחשבי המפתחים עלול להשתמש בפרטי ההזדהות השמורים ב clear text ע"מ להתחבר לנכסי החברה ולסביבת הפיתוח | גישה בלתי מורשית למערכות החברה עלולה  להוביל לנזק מהותי למוניטין החברה ליתרונה העסקי, ולנזק פיננסי בעקבותיו  כמו כן ,  לפגיעה ביכולת לספק שירות ללקוחותיה ע"י פעולות שיבוש מידע או השחתה | בינונית | * שימוש ב Secret manager לצורך שמירה מאובטחת של סיסמאות ופרטי הזדהות נוספים * התקנת EDR על עמדות הקצה ועל שרתי החברה * יש להטמיע בתהליכי התחברות למערכות החברה אימות רב שלבי MFA הכולל שליחת OTP ( One Time Password) באמצעות SMS |
| 5. איבוד מידע רגיש ועסקי עקב אי הגדרת תהליך גיבוי מסודר לסביבת Prod | לא קיים תהליך גיבוי מסודר של שרתי הפיתוח באחריות החברה מידע זה עלול להימחק בעת תקלה | בעת תקלה באחד משרתי הפיתוח הלא מנוהלים ע"י ספק הענן כמו ec2 החברה עלולה לאבד מידע שנצבר בשרתים אלו טרם התקלה , דבר אשר עלול להוביל להפסדים וקושי בחזרה לפעילות עסקית תקינה | בינונית | * יש להגדיר תהליך גיבוי מוסדר לאחר כל שינוי מהותי שמתבצע במערכות כולל נוהל תצורת שינויים וחזרה לאחור * לדוגמא: ניתן ליצור   AMI (Amazon Machine Image) של  שרתי ec2 שמנוהלים ע"י החברה בלבד לאחר כל שינוי מהותי בשרת |
| 6. חשיפת מידע עסקי של החברה בערוצי הדוא"ל או באתרים ציבוריים באמצעות חיבור עם כתובת מייל פרטית | מידע עסקי של החברה עובר בערוצי תקשורת פרטיים כגון gmail פרטי  אין שליטה וניטור מספקים  דבר אשר עלול להקשות על תחקיר בעת אירוע סייבר בערוץ זה | טעות אנוש של אחד מהעובדים עלולה להוביל לשליחת מידע עסקי לגורם חיצוני .  כמו כן , לא קיים ניטור על מערכת הדוא"ל | נמוכה | * יש לעבור לחשבון דוא"ל עסקי הכולל ניטור של מערכת זו ע"מ להקנות יכולות תחקור בעת אירוע סייבר |