סייבר ישראל
משרד ראש הממשלה
מערך הסייבר הלאומי

# תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר

סייבר ישראל
משרד ראש הממשלה
מערך הסייבר הלאומי

# תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר

כל הזכויות שמורות
למערך הסייבר הלאומי

מסמך זה נכתב על-ידי מרכז היערכות לאומית במערך הסייבר הלאומי לטובת הציבור, והוא מומלץ לכלל הארגונים במשק הישראלי לטובת העלאת העמידות והחוסן בסייבר. המסמך מגדיר עקרונות ודרכים לפעולה בנושא היערכות וניהול מצבי משבר במרחב הסייבר האזרחי. הוא כלי לבניית תוכנית סייבר להיערכות ולניהול מצבי משבר, כל ארגון ברמתו, לשמירה על רציפות תפקוד והמשכיות עסקית, וכן מסייע לבחינת מידת ההיערכות הארגונית בנושא. המסמך מיועד למועצות מנהלים (דירקטוריונים), להנהלות של ארגונים, למנהלי הגנה בסייבר והיערכות לחירום ולאחראים לניהול סיכונים, רציפות תפקוד והמשכיות עסקית. המסמך פונה לכלל המשק ונכתב בלשון זכר מטעמי נוחות בלבד. התייחסות למסמך ניתן להעביר במייל ל-preparedness@cyber.gov.il.

# תוכן עניינים

# תקציר מנהלים

העלייה ביכולות התוקפים ובמאמציהם במרחב הסייבר, בד בבד עם התלות הגוברת במערכות מחשוב, מגדילות מאוד את הסבירות להתרחשות משבר סייבר רחב ומתמשך, בעל פוטנציאל נזק אדיר לארגונים, למגזרים (סקטורים) ואף למדינות.

על מנת להתמודד עם משבר סייבר ביעילות, נדרש לבצע היערכות מקדימה, שתאפשר לנהל את המשבר באופן שיקטין את נזקיו והשלכותיו ויקצר את משכו. לפיכך, במסגרת פעולותיו לבניית עמידות וחוסן לאומי בסייבר, מערך הסייבר הלאומי מקדם את נושא ההיערכות בסייבר למצבי משבר. מרכיב מהותי בהיערכות זו הוא **"התפיסה הלאומית בסייבר להיערכות ולניהול מצבי משבר"**, המובאת להלן.

התפיסה היא מסמך יסוד המגדיר עקרונות ודרכים לפעולה בנושא היערכות וניהול מצבי משבר במרחב הסייבר האזרחי. היא מעניקה מסגרת לשפה משותפת ולהעמקת שיתוף הפעולה בסייבר בנושא מצבי משבר, למשרדי הממשלה, לרגולטורים, לארגונים ממלכתיים העוסקים בתחום הסייבר ולכלל המשק.

כמו כן היא כלי לבניית תוכנית סייבר להיערכות ולניהול מצבי משבר, כל ארגון ברמתו, לשמירה על רציפות תפקוד והמשכיות העסקית, וכן מסייעת לבחינת מידת ההיערכות הארגונית בנושא. התפיסה מפרטת את אופן מיפוי "נכסי הסייבר החיוניים", יש בה הסבר על מצבי הכוננות בסייבר ועקרונות לשינוי הכוננות, וכן הרחבה בנושאים של גיבוש "ארגז כלים" להיערכות, תפיסת הניהול של משבר סייבר ופעולות שיסייעו בהתמודדות הולמת עם המשבר.

לנוכח השלכותיו החמורות של משבר סייבר, ומאחר שהוא אינו סוגיה טכנולוגית גרידא, אלא נושא מורכב הדורש מענה של בעלי תפקידים רבים ופיתוח יכולות ארגוניות מתאימות, התפיסה מיועדת למועצות מנהלים (דירקטוריונים) ולהנהלות של ארגונים, שכן הם מחזיקים באחריות הכוללת להיערכות למצבי משבר, וינהלו את המשבר אם יתרחש. התפיסה מיועדת גם למנהלי הגנה בסייבר והיערכות לחירום ולאחראים לניהול סיכונים, רציפות תפקוד והמשכיות עסקית.

התפיסה נכתבה במרכז היערכות לאומית במערך הסייבר הלאומי, בהסתמך על ניסיון וידע שנצברו במערך הסייבר הלאומי ובארגונים מהמגזר הציבורי והפרטי הפועלים בתחום הסייבר בישראל ובחו"ל. על בסיס התפיסה יופצו בעתיד נהלים ושיטות עבודה ויהיו הרחבות מקצועיות בנושא היערכות וניהול מצבי משבר בסייבר, ואלה יסייעו במימוש התפיסה ובהטמעתה במשק.

# הגדרות ומושגים

ההגדרות והמושגים להלן מתבססים על "מילון מונחי הסייבר"[1] שגובש במערך הסייבר הלאומי, וכן על החלטות ממשלה ומסמכים העוסקים בהיערכות למצבי חירום, ונוסחו בהתאם למסמך זה.

**מרחב הסייבר הגלובאלי (Global Cyberspace):** המארג של תשתיות המידע הטכנולוגיות, הכולל את האינטרנט, רשתות התקשורת, מערכות המחשוב וכל המעבדים והבקרים הממוחשבים המשובצים במערכות טכנולוגיות, והמשתמשים של כל אלה.

**מרחב הסייבר האזרחי של מדינת ישראל (Israel's Civil Cyberspace):** מרחב הסייבר של כלל הגורמים הממלכתיים והפרטיים במדינת ישראל, למעט הגופים המיוחדים (צה"ל, משטרת ישראל, שב"כ, המוסד ומערכת הביטחון).

**נכס סייבר (Cyber Asset):** מערכת תקשוב (לרבות חומרה ותוכנה), המשמשת בין היתר לאחסון, ניהול, עיבוד והעברה של מידע, ו/או לתפעול, שליטה ובקרה.

**נכס סייבר חיוני (Vital Cyber Asset):** נכס סייבר שתפקודו התקין נדרש לשמירת רציפותו של תהליך ליבה.

**תהליך ליבה (Core Process):** תהליך שמבצע ארגון על מנת לממש את יעדיו המרכזיים ו/או יעדים שהוגדרו לו.

**שגרת הגנה בסייבר (Cyber Routine):** מצב שבו לא מסתמן נזק לתפקודם התקין של נכסי סייבר חיוניים.

**אירוע סייבר (Cyber Incident):** התרחשות המעידה על פגיעה אפשרית בפעילותו התקינה של נכס סייבר, שיש יסוד להניח כי היא נובעת מפעילות מכוונת במרחב הסייבר.

**משבר סייבר (Cyber Crisis):** מצב שיש בו איום ממשי לפגיעה בנכס סייבר חיוני, או פגיעה בו בפועל, אשר עלול לגרום נזק קריטי לשגרת הפעילות ולתדמית, נזק כלכלי ופגיעה בחיי אדם. משבר סייבר נע במדרג רמות חומרה, ובמצב קיצון נגרם נזק ניכר לתהליכי ליבה ולרציפות התפקוד הארגונית/המשקית, והוא עלול להסלים עד כדי מצב חירום לאומי.

**מחולל חירום (Emergency Trigger):** מהלך מלחמתי, תופעת טבע, משבר סייבר, פעולת טרור, תקלה וכיו"ב, שרמת הסיכון הטמונה בו מוערכת כעלולה לחולל מצב חירום.

**מצב חירום לאומי (National State of Emergency):** מצב קשה ומסוכן ובו סיכון ממשי לפגיעה בציבור ו/או בחוסנה הלאומי של המדינה, המצריך פעילות רב תחומית ברמה הלאומית, לרבות הכרזה על-פי דין (לדוגמה "מצב מיוחד בעורף", "אירוע חירום אזרחי", הכרזת מלחמה).

**מצב כוננות לאומי (National State of Alert)[2]:** נובע מאפשרות התרחשות מצב חירום שתוצאותיו חוצות ארגונים. העלאת מצב הכוננות הלאומי נועדה להקטין את הסבירות להתרחשות אירוע ואת פוטנציאל הנזק מהתרחשותו. מצב הכוננות הלאומי משפיע בהכרח על מצב הכוננות בסייבר.

**מצב כוננות בסייבר (Cyber State of Alert):** קביעה רשמית של רמתה, מהותה והיקפה של ההיערכות הנדרשת בסייבר להתמודדות עם הנסיבות. מצב הכוננות בסייבר עשוי להשפיע על מצב הכוננות הלאומי.

---

1 את המילון אפשר למצוא באתר האינטרנט של מערך הסייבר הלאומי, בכתובת: https://www.gov.il/he/Departments/General/terms

2 המונחים "מצב חירום לאומי" ו"מצב כוננות לאומי" טרם הוגדרו בחוק

# מבוא

## 1. המאמץ להגנת מרחב הסייבר האזרחי

בעשור החולף אנו עדים להתפתחותו האדירה של מרחב הסייבר ולמגוון ההזדמנויות והאפשרויות שהוא מציע. בה בעת, הצמיחה המואצת של טכנולוגיות תקיפה והתגברות התלות בשימוש במערכות ממוחשבות, הובילו להפיכתו של מרחב הסייבר לתווך נרחב לפעילויות עוינות בעצימות גוברת ובהיקפים גדלים. נכסי סייבר, בדגש על תשתיות קריטיות, נעשו מטרה איכותית לתקיפות, מספר המטרות וסוגיהן גדל והולך, ועקב כך גם הסכנה הנשקפת לפרטים, לארגונים, למגזרים (סקטורים) ולמדינות.

על-פי איום ותרחיש הייחוס המצרפי לזירה האזרחית, שאישר הקבינט המדיני-ביטחוני בהחלטה ב/120[3], הסייבר הוא מחולל חירום מרכזי, ועלול להוביל למצב חירום לאומי. בהתאם קבעה הממשלה בהחלטות 3611[4] ו-2444[5] את הצורך בגיבוש תפיסה לאומית לטיפול במצב חירום במרחב הסייבר, וכי ההגנה על תפקודו התקין והבטוח של מרחב זה נדרשת בשגרה ובחירום, והיא יעד ואינטרס לאומי ממלכתי חיוני לביטחונה של מדינת ישראל.

לנוכח הפוטנציאל הנפיץ של איום הסייבר והנחיות הממשלה בנושא, מערך הסייבר הלאומי, בשיתוף ובסיוע משרדי הממשלה, רגולטורים וארגונים ממלכתיים אחרים, מוביל מאמץ להגנת מרחב הסייבר האזרחי ולשמירתו כמרחב בטוח. במוקד המאמץ ננקטות פעולות להנחיה ולהכוונת הארגונים במשק, על בסיס ההבנה כי במקרים רבים הם מושא התקיפה בסייבר ותווך שבו היא עוברת לארגונים אחרים. הפעולות באות לידי ביטוי בין היתר בהגברת המודעות לאיומים, בהנחלת נורמות, ובמתן כלים לניהול ולטיוב ההגנה מפני אירועי סייבר ולצמצום פוטנציאל התממשותם.

## 2. החשיבות בהיערכות למצבי משבר בסייבר והנחות יסוד

רוב אירועי הסייבר מקבלים מענה מספק על-ידי צוותי התגובה הטכנולוגיים הארגוניים, ואינם גורמים לנזק משמעותי וארוך טווח.

3 החלטת ועדת השרים לענייני ביטחון לאומי (הקבינט המדיני-ביטחוני), מיום 15 ביוני 2016
4 החלטת ממשלה 3611 מיום 07 באוגוסט 2011, בנושא "קידום היכולת הלאומית במרחב הקיברנטי"
5 החלטת ממשלה 2444 מיום 15 בפברואר 2015, בנושא "קידום ההיערכות הלאומית להגנת הסייבר"

אולם מתקפות סייבר שהתרחשו ברחבי העולם והנזקים המשמעותיים וארוכי הטווח שגרמו, המחישו כי נדרש לפתח מענה שונה ויכולות מקיפות יותר, מעבר להטמעת טכנולוגיות הגנה ולפעולות להבטחת שגרת הפעילות באיומי סייבר ולהתמודדות עם אירוע סייבר נקודתי. על כן נדבך משלים למאמץ להגנת מרחב הסייבר האזרחי הוא ההיערכות בסייבר למצבי משבר, שתסייע לצמצם את הסבירות להפיכת אירוע סייבר למשבר סייבר, ואם התממש המשבר תעזור לנהל אותו ביעילות.

בבסיס התפיסה שתי הנחות יסוד המדגישות את החשיבות שההיערכות בסייבר תעשה אל מול הנסיבות השוררות הן במרחב הסייבר והן במרחב הפיזי:

1. משבר סייבר עלול לגרום נזק של ממש ופגיעה ברציפות התפקוד, ולהסלים עד כדי מצב חירום לאומי. כך למשל, בדצמבר 2015 התרחשה מתקפת סייבר נגד רשת החשמל של אוקראינה, ושיבשה את אספקת החשמל למאות אלפי בתי אב למשך כמה שעות. באירוע אחר, במאי 2017, פגעה קשות מתקפת הסייבר הבין-לאומית "WannaCry" במערך המחשוב של שירות הבריאות הלאומי בבריטניה. בשני האירועים הייתה הפגיעה בנכסי סייבר חיוניים, והעידה על קפיצת המדרגה בתעוזת התוקפים ועל התעצמות איום הסייבר.

2. מצבי חירום שנגרמו ממחולל פיזי שאינו סייבר (לדוגמה: מלחמה, טרור, תופעת טבע וכיו"ב) מגדילים את הסבירות להתרחשות משבר סייבר, מכיוון שיתעצמו בהם מאמצי התוקף בסייבר[6] ובד בבד תגבר התלות בתפקודם התקין של נכסי סייבר חיוניים[7]. כך למשל, במהלך העימות בין גיאורגיה ורוסיה שהחל באוגוסט 2008, ובסמוך אליו, נתקפו בסייבר ושותקו אתרי הממשל והתקשורת של גיאורגיה ורשת הטלפונים קרסה. תקיפת סייבר נוספת גרמה לפיצוץ בצינור המוביל נפט דרך גיאורגיה לאירופה (BTC), שלו תרומה אדירה לכלכלת המדינה. דוגמה אחרת הייתה במבצע "צוק איתן", באוגוסט 2014, במהלכו נאלצה ישראל להתמודד עם מתקפת סייבר על מטרות צבאיות ואזרחיות, שהתגברה ככל שהפעילות הצבאית הורחבה והועמקה.

### 3. מטרות התפיסה וקהל יעד

התפיסה נובעת מההבנה כי ההיערכות והניהול של מצבי משבר מחייבים שילוב כוחות, תיאום ושיתוף פעולה ברמה הלאומית, ורק כך ישיגו את תכליתם. התפיסה מיועדת אפוא למשרדי הממשלה, לרגולטורים ולארגונים ממלכתיים העוסקים בתחום הסייבר, מכיוון שהם מובילים את המאמץ המדינתי המגננתי להכלת התקיפות והשלכותיהן ומנחים ומכוונים את ארגוני המשק. התפיסה נגישה ומומלצת לארגוני המשק

6 התוקף ישאף לייצר מרחב נוסף שיהיה צורך לתת לו מענה, או לחלופין לנצל הזדמנות שתשומת הלב מוסטת עקב מצב החירום המתחולל. מכאן נובע שמשבר סייבר עשוי להתחולל בו בזמן שמתרחש משבר מסוג אחר

7 לדוגמה נכסי סייבר שתומכים בשירותים קיומיים ומאפשרים את המשך מרקם החיים ואת רציפות תפקוד המשק החיוני

בכללותם, כדי שיסתייעו בה ויכירו את הפעולות שנעשות ברמה הלאומית.

**מטרת התפיסה:**

1. לשמש מסמך יסוד המגדיר עקרונות ודרכים לפעולה בנושא היערכות וניהול מצבי משבר במרחב הסייבר האזרחי.

**מטרות משנה:**

1.1. לייצר שפה משותפת ולהיות בסיס להעמקת שיתוף הפעולה והשיח בסייבר בנושא מצבי משבר, הן בין גורמים מדינתיים והן עם גורמים פרטיים.

1.2. לשמש כלי מסדר ומכוון לבניית תוכנית סייבר להיערכות ולניהול מצבי משבר, כל ארגון ברמתו, לשמירה על רציפות התפקוד וההמשכיות העסקית, ולסייע בבחינת מידת ההיערכות הארגונית בנושא.

1.3. לשמש בסיס למערך הסייבר הלאומי ולגורמים נוספים, לפיתוח עזרים עתידיים בנושא היערכות וניהול מצבי משבר בסייבר, דוגמת נהלים ושיטות עבודה, הרחבות מקצועיות ותהליכים. כל אלה יסייעו ביישום התפיסה ובהטמעתה במשק.

מאחר שמשבר סייבר עלול לפגוע קשות בשמו הטוב של הארגון, בנכסיו, בתפקודו או ביכולותיו להשיג את יעדיו המרכזיים (עד כדי סיכון עצם קיומו), ומכיוון שהוא מצריך התייחסות בקשת רחבה של היבטים ארגוניים ועסקיים, ההיערכות למשבר וניהולו הם באחריות הדרג הבכיר בארגון. על כן נכתבה התפיסה למועצות מנהלים (דירקטוריונים) ולהנהלות של ארגונים. התפיסה מיועדת גם לדרג המקצועי, בדגש על מנהלי ההגנה בסייבר והיערכות לחירום ולאחראים לניהול סיכונים, רציפות תפקוד והמשכיות עסקית.

# מיפוי נכסי הסייבר החיוניים

## 1. על מה נדרש להגן

שגרת היומיום רוויה באיומי סייבר ובתקיפות של נכסי סייבר, ובמרבית המקרים מאמצי ההגנה מכילים את התקיפות ומאפשרים המשך פעילות. למרות זאת מקרים שבהם התוקפים בסייבר מצליחים במאמציהם, אם מכיוון שהתגברו על מערכות ההגנה הקיימות או ניצלו את הגורם האנושי[8], אינם תרחיש חריג. מקרים כאלה יכולים להתפתח למשבר סייבר, בייחוד כשהפגיעה היא בנכסי סייבר חיוניים, ועלולה לגרום נזק קריטי לשגרת הפעילות ולתדמית, נזק כלכלי ופגיעה בחיי אדם. על כן איום ממשי לפגיעה בנכס סייבר חיוני, או פגיעה בו בפועל, הם בסיס לזיהוי מצבי משבר בסייבר ולבחינת רמת חומרתם.

כדי למזער את הסבירות להתרחשות משבר סייבר ולשם גיבוש מענה הולם שיקטין את נזקיו והשלכותיו, תוך הגדרה וניצול יעיל של משאבים ויכולות, בשלב הראשון על כל גורם למפות את נכסי הסייבר החיוניים הרלוונטיים בעבורו. אלה הם נכסי סייבר שתפקודם התקין נדרש לשמירת רציפות התפקוד של תהליכי ליבה שהוא מנהל.

בהתאם לתורת ההגנה בסייבר לארגון (תוה"ג)[9] שפותחה במערך הסייבר הלאומי, על ההגנה להיות מותאמת לפוטנציאל הנזק, כלומר ההשקעה בהגנה על כל נכס תהיה בהתאם לרמת הקריטיות שלו, לתפקוד הארגון וליעדים שהוא משרת, או שהוגדרו לו. על כן עיקר ההשקעה בהגנה צריכה להיות על נכסי הסייבר החיוניים. מצד התוקף נכסים אלה הם יעד אטרקטיבי לתקיפות סייבר ולכן האיום הנשקף מהם גדול.

## 2. אופן מיפוי נכסי הסייבר החיוניים

ברמת הארגון, באמצעות המתודולוגיה שבתוה"ג, כל ארגון יכול למפות באופן יעיל ונכון את נכסי הסייבר החיוניים שהוא מחזיק בהם ולדרג אותם לפי סדר חשיבות, לעשות הערכת סיכונים לנכסים ולבנות תוכנית להגדלת רמת ההגנה עליהם בסייבר.

ברמה הלאומית[10], שהיא מוקד התפיסה המובאת במסמך זה, שני צירים מרכזיים למיפוי נכסי סייבר חיוניים הם עבודה שנעשית במערך הסייבר הלאומי בתהליך Bottom-Up (מטה-מעלה) וכן עבודה של רשות חירום לאומית (רח"ל) ומשרדי הממשלה בתהליך Top-Down (מעלה-מטה):

**2.1. הגדרת נכסי סייבר חיוניים Bottom-Up:** בציר זה ההסתכלות מתחילה מלמטה. מערך הסייבר הלאומי בוחן את תהליכי הליבה בארגונים במשק, ומזהה נכסי סייבר שתפקודם התקין נדרש לשמירת הרציפות של תהליכי הליבה. לאחר מכן נבחנים נכסי הסייבר שזוהו אל מול תבחינים שגובשו במערך הסייבר, אשר משמשים מנגנון מיפוי פרואקטיבי להגדרת ארגונים שפגיעה בהם בסייבר עלולה להסב נזק ניכר למדינת ישראל. נכסי סייבר שנמצאו עומדים בתבחינים מוגדרים נכסי סייבר חיוניים, בחלוקה לשני סוגים של ארגונים:

א. ארגון מונחה תמ"ק (תשתית מדינה קריטית): ארגון שמחזיק בנכס סייבר שנמצא עומד ברף הגבוה ביותר של התבחינים, מובא לדיון בוועדת ההיגוי להגנה על מערכות ממוחשבות חיוניות בראשות ראש מערך הסייבר הלאומי[11]. תפקידה בין היתר הוא לבחון אילו ארגונים נדרשים להיות מוגדרים "קריטיים" ולכן זקוקים לרמה

8 למשל באמצעות מתקפת "דיוג" (Phishing)

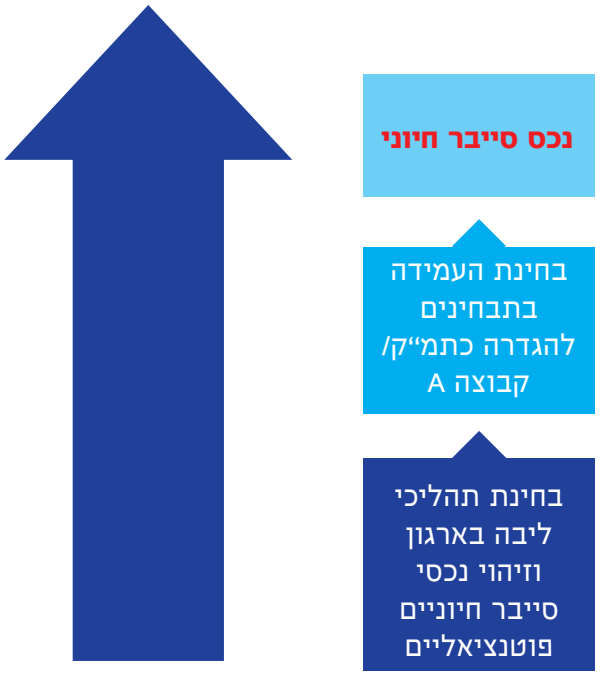
9 את התוה"ג ניתן למצוא באתר האינטרנט של מערך הסייבר הלאומי, בכתובת:
https://www.gov.il/he/Departments/Policies/cyber_security_methodology_for_organizations

10 מיפוי נכסי סייבר חיוניים ברמה הלאומית נעשה בהובלה ובסיוע של ארגונים ממלכתיים העוסקים בתחום הסייבר, משרדי הממשלה ורגולטורים. מדובר בנכסי סייבר שנדרשים להבטחת רציפות התפקוד הלאומית ושגרת החיים, ופגיעה בהם עלולה להסב נזק ממשי למדינת ישראל

11 ועדת ההיגוי הוקמה בעקבות החלטת ממשלה ב/84 מיום 19 בדצמבר 2002, בנושא "אחריות להגנה על מערכות ממוחשבות חיוניות"

גבוהה של הגנה בסייבר. ארגונים שאושרו בוועדת ההיגוי ובהמשך גם בוועדת הפנים והגנת הסביבה של הכנסת, מונחים מתוקף חוק[12] ישירות על-ידי אגף תמ"ק במערך הסייבר הלאומי, או באמצעות יחידה ייעודית של שירות ביטחון כללי (שב"כ).

ב. ארגון "קבוצה A": פרט לארגונים מונחי תמ"ק, כדי לבנות יכולת אפקטיבית להגדלת רמת החוסן של המשק האזרחי בפני איומי סייבר, מערך הסייבר הלאומי פועל להגדיר קבוצות מיקוד שונות במשק, וכל אחת מהן תקבל הנחיה דיפרנציאלית. רוב משאבי ההנחיה יוקצו לקבוצת ארגונים קטנה במשק (מאות ארגונים), להלן "קבוצה A", על בסיס ההבנה שהם מחזיקים בנכסי סייבר חיוניים שמשקלם בתהליכים המרכזיים במשק גדול מאוד, ותקיפתם בסייבר עלולה לגרום נזק רב.




הגדרת נכסי הסייבר החיוניים BOTTOM-UP

12 חוק להסדרת הביטחון בגופים ציבוריים (הוראת שעה), התשע"ו-2016

**2.2. הגדרת נכסי הסייבר החיוניים Top-Down:** ציר נוסף להגדרת נכסי הסייבר החיוניים ברמה הלאומית קשור בעבודה שעושים רשות חירום לאומית (רח"ל) ומשרדי הממשלה בתחום רציפות תפקוד המשק. בציר זה ההסתכלות מתחילה מלמעלה, שכן ראשיתו ביעדי השירות הלאומיים, שהם ההגדרות המעשיות של שירותים ותפקודים של מערכות אשר יש להמשיך ולקיים גם במצבי משבר, כדי להבטיח את רציפות התפקוד הלאומית ואת שגרת החיים בעורף[13].

כנגזרת מיעדי השירות הלאומיים ועל מנת לאפשר את קיומם, רח"ל פועלת מול משרדי הממשלה להגדרת יעדים משרדיים ורמות שירות, שהם ההגדרות המעשיות והכמותיות של יכולות תפקודיות במשרדי הממשלה והארגונים בתחומי אחריותם אותן נדרש לשמר ככל שאפשר גם במצבי משבר.

עמידה ביעדים וברמות השירות שהגדירו משרדי הממשלה, מחייבת מימוש של תהליכי ליבה המתנהלים בארגוני המשק, ורציפות התפקוד של רבים מהם תלויה בנכסי סייבר. בסיוע שאלון מיפוי שגובש במערך הסייבר הלאומי[14], נדרש כל רגולטור לעבוד עם הארגונים שבאחריותו כדי לזהות את נכסי הסייבר הללו, והם יוגדרו נכסי סייבר חיוניים ויידרשו ברמה גבוהה של הגנה בסייבר.

**2.3. שרשרת האספקה:** שלב חשוב בתהליך מיפוי נכסי הסייבר החיוניים וההגנה עליהם, בכל אחד מהצירים שתוארו לעיל, הוא בחינת שרשרת האספקה. פעילותם של ארגונים רבים תלויה בשירותים שהם רוכשים או מקבלים מספקים חיצוניים, למשל קבלני משנה שמייצרים רכיבים ממוחשבים, ספקים של שירותי מחשוב ועוד. שירותים אלה יכולים להיות בעלי קישוריות אל מערכות הארגון, ולכן גם אל נכסי הסייבר החיוניים. על כן כל ארגון נדרש למפות ולזהות את האיומים והסיכונים שיש במערכות ובשירותים של הספק ולגלמם בהשקעה בהגנה על נכסי הסייבר החיוניים.


13 לדוגמה קיום מזון ומשקה ראויים, הספקת שירותי רפואה, יציבות המערכת הכלכלית וכיו"ב
14 ראה נספח א'

# מצבי הכוננות בסייבר ועקרונות לשינוי רמת הכוננות

### 1. כללי

מצבי הכוננות בסייבר מהווים שפה משותפת לשיקוף מידת הדריכות וההיערכות הנדרשת אל מול הנסיבות השוררות במרחב הסייבר האזרחי ובמרחב הפיזי, ולקראת התרחשויות אפשריות בהם. הם ייקבעו כפוף להערכת מצב, שנועדה לסייע בפיתוח הבנת המשמעות של המתרחש על בסיס מידע ועובדות וחשיבה משותפת, ולאחר מכן הגדרת פעולות לביצוע. הכרזה על מצב כוננות סייבר התואם את המציאות ואת גודל האיום, והפעולות שיבוצעו בהתאם, יסייעו להקטין את הסבירות לפגיעה בנכסי סייבר חיוניים ולהתפתחות משבר סייבר, ואם כבר קרו - לצמצום הנזק שנגרם. לעומת זאת, אי הכרזה על מצב כוננות תואם תגרום נזק בהיקף רחב, נזק שהיה אפשר למנוע או לכל הפחות לצמצם.

### 2. סרגל החומרה: רמזור

כל עוד לא הוכרז אחרת ארגון נמצא במצב של "שגרת הגנה", מבצע פעילות הקשורה בהתנהלותו השוטפת ומתכונן למצבי משבר[15]. במצב זה לא מסתמן נזק לתפקודם התקין של נכסי סייבר חיוניים של הארגון. איום ממשי לפגיעה בנכס סייבר חיוני, או פגיעה אפשרית בפעילותו התקינה (גם אם טרם הוכח כי היא נובעת מאירוע סייבר), הם ביטוי להסלמה ומגבירים את הסבירות להתרחשות משבר סייבר. במצב קיצון מתחוללת פגיעה רחבה וממושכת בנכס/י סייבר חיוני/ים של הארגון, וגורמת נזק ניכר לתהליכי ליבה ולרציפות התפקוד הארגונית (המשכיות עסקית).

## סרגל החומרה: רמזור

**(מה קורה במערכות הארגון בזמן נתון)**

| מצב | תיאור |
|---|---|
| **שגרת הגנה** | ירוק: מצב שבו לא מסתמן נזק לתפקודם התקין של נכסי סייבר חיוניים |
| **ביטוי להחמרה במצב מערכות הארגון** | צהוב: איום ממשי לפגיעה בנכס סייבר חיוני, או פגיעה אפשרית בפעילותו התקינה |
| | אדום: פגיעה בנכס/י סייבר חיוני/ים, שבגינה קיימת אפשרות לפגיעה משמעותית ברציפותו של תהליך ליבה |
| | שחור: פגיעה רחבה וממושכת בנכס/י סייבר חיוני/ים המובילה לנזק משמעותי לתהליכי ליבה ולרציפות התפקוד הארגונית (המשכיות עסקית) |

15 כפי שיפורטו בהמשך בפרק "היערכות למצבי משבר"

## 3. תבחינים לקביעת מצב הכוננות בסייבר: מה קורה במרחב הסייבר ובמרחב הפיזי

מצב הכוננות בסייבר יוגדר על-פי חומרת התבחינים והסבירות להתרחשותם, ובכך יסומן הצורך בהפעלה ובשימוש במשאבים ובכלים, ויוערך היקפם. מכיוון שבמצבי חירום שנגרמו ממחולל שאינו סייבר (לדוגמה מהלך מלחמתי, תופעת טבע, פעולת טרור, תקלה וכיו"ב) סביר שיתגברו מאמצי התוקף בסייבר, ובד בבד עולה חשיבות תפקודם התקין של נכסי סייבר חיוניים התומכים בתהליכי ליבה, מצב הכוננות בסייבר ייקבע לא רק לנוכח המצב במרחב הסייבר, אלא גם לנוכח המצב במרחב הפיזי[16].

שני דגשים חשובים בהקשר של המתאם (קורלציה) בין התבחינים ובין מצבי הכוננות:

א. התממשותו של תבחין מסוים לא מכתיבה בהכרח קביעה של רמת כוננות סייבר ספציפית, אלא התבחינים הם כלי עזר להחלטה על הכוננות כפוף להערכת מצב.

ב. העלאת הכוננות בסייבר תיתכן גם טרם התרחש אירוע סייבר וכאשר אין ביטוי לפגיעה בנכסי סייבר חיוניים, למשל בעקבות מידע התרעתי או עקב התרחשויות שמגבירות את התלות בהם ואת חשיבות תפקודם התקין. כלומר ארגון יכול להיות במצב כוננות א' או ב' ובו-זמנית להיות במצב "ירוק" בסרגל החומרה.

להלן פירוט מצבי הכוננות בסייבר והתבחינים לקביעת כל אחד מהם:

### 3.1. מצב שגרת הגנה בסייבר

זהו מצב ברירת המחדל, ובו ההתרחשויות במרחב הסייבר ובמרחב הפיזי לא מצביעות על נזק לתפקודם התקין של נכסי סייבר חיוניים, או על הצורך בהגברת ההגנה עליהם. במצב זה אין ביטוי לתבחינים ברמות כוננות גבוהות יותר.

תבחינים במרחב הסייבר: ללא התרחשות, או התרחשות אירועי סייבר שפוגעים בפעילותם התקינה של נכסי סייבר, אולם ללא פגיעה בנכסי סייבר חיוניים.

תבחינים במרחב הפיזי: ללא התרחשות או התרעות כלליות לאירוע ביטחוני.

### 3.2. מצב כוננות סייבר א'

מצב כוננות סייבר א' ייקבע כפוף להערכת מצב[17] וכאשר מתממש לפחות אחד מהתבחינים האלה:

תבחינים במרחב הסייבר: התרחשות אירוע סייבר שבו מסתמנת פגיעה אפשרית בתפקודו התקין של נכס סייבר חיוני; קבלת מידע התרעתי; התרחשות אירוע סייבר מתוזמן (לדוגמה "OpIsrael")[18]; התרחשות אירוע בחו"ל שטרם התפשט לישראל (לדוגמה "WannaCry"); אירוע סייבר המיוחס לישראל.

תבחינים במרחב הפיזי: תקלה תפעולית/טכנית בנכס סייבר חיוני ו/או במתקן המחזיק בו; התרעה לאירוע ביטחוני רחב היקף; התרחשות אירוע ביטחוני חריג (לדוגמה התגברות ירי לעבר ישראל, התרחשות תקיפה המיוחסת לישראל);

16 כפי שהוסבר בסעיף הנחות היסוד בפרק "מבוא"
17 להרחבה על הערכת המצב בסייבר, ראה נספח ב'
18 מתקפת סייבר שנתית המכוונת נגד ישראל, שהתרחשה לראשונה באפריל 2013

העלאת רמת כוננות בצה"ל; התרחשות אירוע חריג שעלולה להיות לו השפעה על מרחב הסייבר.

### 3.3. מצב כוננות סייבר ב'

מצב כוננות סייבר ב' ייקבע כפוף להערכת מצב וכאשר מתממש לפחות אחד מהתבחינים האלה:

תבחינים במרחב הסייבר: מידע התרעתי ממשי להתארגנות לתקיפה; פגיעה בנכס/י סייבר חיוני/ים ובעקבות זאת אפשרות לפגיעה ממשית ברציפותו של תהליך ליבה.

תבחינים במרחב הפיזי: פגיעה פיזית בשירותים חיוניים למשק (לדוגמה: הספקת חשמל, שירותי בריאות); התרחשות אירוע ביטחוני נרחב (לדוגמה: ירי רחב היקף, מבצע צבאי מוגבל).

### 3.4. מצב כוננות סייבר ג'

מצב כוננות סייבר ג' הוא המצב הגבוה ביותר של כוננות בסייבר, וההתרחשויות שבגינן הוכרז

## מצבי הכוננות בסייבר

עלולות להסלים עד כדי מצב חירום לאומי. מצב כוננות סייבר ג' ייקבע כפוף להערכת מצב וכאשר מתממש לפחות אחד מהתבחינים האלה:

תבחינים במרחב הסייבר: פגיעה רחבה ו/או ממושכת בנכס/י סייבר חיוני/ם, המובילה לנזק ניכר לתהליכי ליבה ולרציפות התפקוד של המשק (לדוגמה: פגיעה חוצת מגזרים).

תבחינים בממד הפיזי: פגיעה פיזית רחבה ו/או ממושכת בשירותים חיוניים למשק; מלחמה או מבצע צבאי רחב היקף; הכרזה על "מצב מיוחד בעורף"/"אירוע חירום אזרחי".

### 4. עקרונות לשינוי רמת הכוננות בסייבר

במסגרת כל אחד ממצבי הכוננות יבצע ארגון ברמתו הערכת מצב, יבחן את התבחינים במרחב הסייבר ובמרחב הפיזי, ובהמשך ייבחן הצורך בשינוי הכוננות.

**4.1. העלאת רמת הכוננות בסייבר:** המעבר לרמת כוננות סייבר גבוהה יותר נובע מאפשרות ממשית להסלמה בנסיבות השוררות או הסלמה בפועל, שמחייבת נקיטת פעולות שטרם ננקטו או הגדלה מתונה ככל האפשר בעצימות ובהיקף הפעולות שכבר ננקטו. פעולות אלו נועדו למנוע החמרה נוספת, או לפחות למזער את הנזק שייגרם. העלאת רמת הכוננות תיעשה בהתאם לתבחינים ובהדרגה, אולם לא בהכרח. כך למשל, במצב קיצון ייתכן כי יוכרז מצב כוננות סייבר ג' לפני שהוגדר מצב כוננות אחר.

**4.2. הורדת רמת הכוננות בסייבר:** המעבר לרמת כוננות נמוכה יותר ייעשה אם התבחינים שהובילו לקביעת רמת הכוננות חדלו מלהתקיים. הורדת רמת הכוננות תיעשה בהדרגה, כלומר ברמת כוננות אחת בכל פעם, עד לחזרה למצב שגרת הגנה בסייבר.

### 5. צירים להכרזה על מצב הכוננות בסייבר

לאור המתודולוגיה שהוצגה לעיל, יש שלושה צירים מרכזיים להכרזה על מצב הכוננות במרחב הסייבר האזרחי: ברמה הלאומית, ברמת מגזרי המשק[19] וברמת הארגון. לנוכח החשיבות הרבה בשיתוף מידע בסייבר ובהתחשב במהירות שבה מתרחשים אירועי סייבר, חיוני שכל גורם העושה שינוי בכוננות יעדכן על כך את כלל הגורמים הרלוונטיים, לרבות מערך הסייבר הלאומי, הרגולטור וארגונים מונחים (אם יש כאלה). לרוב ייעשה העדכון בחשאיות, וזו תאפשר לבצע "הגנה שקטה", כלומר מענה לאירוע הסייבר תוך כדי הקפדה על הסתרת פעולות המגן, כדי להכיל את המתקפה וללמוד את פעילותו ושיטותיו של התוקף.

א. ברמה הלאומית, על מצב הכוננות בסייבר יכריז ראש מערך הסייבר הלאומי, כמי שעומד בראש הארגון הממלכתי האמון על הגנת מרחב הסייבר האזרחי, או בעל תפקיד שהסמיך לכך. כוננות סייבר זו מוכרזת בעקבות איום או התרחשות העלולים להסלים עד כדי מצב חירום לאומי. הכוננות בסייבר ברמה הלאומית מחייבת את כלל מגזרי המשק. מגזר יכול להגדיר לעצמו רמת כוננות סייבר גבוהה מזו שהוגדרה ברמה הלאומית, אולם לא נמוכה ממנה.

מכיוון שבנקודת זמן נתונה מגזרים וארגונים עשויים להיות מושפעים מתבחינים בצורה שונה, וכן להפיק מהערכת המצב משמעויות שונות, פרט לרמה הלאומית יש עוד שני צירים להגדרת מצב הכוננות בסייבר, המבטאים סקטוריאליות ודיפרנציאליות אפשריות:

ב. ברמת המגזר, על מצב הכוננות בסייבר יכריז מנכ"ל המשרד הממשלתי/הגורם הרגולטורי הרלוונטי או בעל התפקיד שהסמיך לכך,

19 מגזר: כלל הגופים הפועלים במסגרת תחום מקצועי של משרד ממשלתי ובמסגרת אחריותו הרגולטורית (מתוך החלטת ממשלה 2443 מיום 15 בפברואר 2015, בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר")

בתיאום עם מערך הסייבר הלאומי או בעקבות המלצתו. ההכרזה מחייבת את כלל ארגוני המשק שבאחריות המגזר[20], או לחלופין ארגונים ספציפיים שהוגדרו נדרשים לכוננות. הכרזה על מצב כוננות סייבר במגזר מסוים אינה מחייבת מגזרים אחרים, אולם היא מסמנת נסיבות השוררות במרחב שאליהן חשוב להתייחס.

ג. ברמת הארגון, על מצב הכוננות בסייבר יכריז מנכ"ל הארגון או בעל התפקיד שהסמיך לכך, בתיאום עם יחידת הסייבר המגזרית[21] ו/או הגורם הרגולטורי, או בעקבות המלצתם/הנחייתם. ארגון יכול להגדיר לעצמו רמת כוננות גבוהה מזו שהוגדרה במגזר שאליו הוא שייך, אולם לא נמוכה ממנה.

# עקרונות לשינוי רמת הכוננות בסייבר וצירים להכרזה

| מצב כוננות סייבר | רמת הארגון | רמת המגזר | רמה לאומית | קריטריונים לירידה ברמת הכוננות |
|---|---|---|---|---|
| ג' | הארגון, תוך תיאום עם יחידת הסייבר המגזרית/ הרגולטור, או לאור המלצתם | המשרד הממשלתי או הרגולטור, תוך תיאום עם מערך הסייבר הלאומי, או לאור המלצתו | מערך הסייבר הלאומי | רציפות התפקוד המשקית הוחזרה לסדרה |
| ב' | הארגון, תוך תיאום עם יחידת הסייבר המגזרית/ הרגולטור, או לאור המלצתם | המשרד הממשלתי או הרגולטור, תוך תיאום עם מערך הסייבר הלאומי, או לאור המלצתו | מערך הסייבר הלאומי | הוסר האיום לפגיעה ברציפות התפקוד ובתהליכי ליבה. רמת האיומים כללית |
| א' | הארגון, תוך תיאום עם יחידת הסייבר המגזרית/ הרגולטור, או לאור המלצתם | המשרד הממשלתי או הרגולטור, תוך תיאום עם מערך הסייבר הלאומי, או לאור המלצתו | מערך הסייבר הלאומי | התבחינים להכרזה על מצב כוננות סייבר א' אינם מתקיימים |
| שגרת הגנה | | | | |

20 חריגים הם ארגוני תמ"ק המופיעים בתוספת לחוק להסדרת הביטחון בגופים ציבוריים, אשר מונחים ישירות בהיבטי סייבר על-ידי מערך הסייבר הלאומי או על-ידי יחידה ייעודית של שב"כ

21 יחידת סייבר מגזרית פועלת בכפיפות למשרד הממשלתי שאליו היא שייכת, והינה יחידה להכוונה מקצועית בתחום הגנת הסייבר של הארגונים שכלפיהם יש למשרד הממשלתי סמכויות רגולציה. היחידה מונחית מקצועית על-ידי מערך הסייבר הלאומי (מתוך החלטת ממשלה 2443 מיום 15 בפברואר 2015, בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר")

# היערכות למצבי משבר: ארגז הכלים (TOP 5)

לנוכח כל אחד ממצבי הכוננות בסייבר שתוארו לעיל, ינקוט כל ארגון ברמתו פעולות שיסייעו להקטין את הסבירות להתפתחות משבר סייבר, או לנהלו באופן שיפחית ככל הניתן את נזקיו והשלכותיו אם כבר התרחש. מדובר במימוש, לעיתים בפרק זמן קצר, של פעולות שבשגרת הגנה בסייבר מבוצעות באופן מצומצם, או שאינן מבוצעות כלל. על כן ככל שרמת הכוננות גבוהה יותר, יידרשו פעולות בעצימות ובהיקפים גדולים יותר[22].

כדי שארגון יוכל לבצע את הפעולות הנדרשות בזמן ניהול משבר, עליו להיערך אליהן כבר בשלב שגרת ההגנה. פעולות שלא יוכנו בעוד מועד לא יהיה אפשר לבצע בזמן משבר, או יהיה אפשר לבצען חלקית, באיחור ולא באופן מיטבי. לשם כך, נדבך משמעותי בהיערכות בסייבר למצבי משבר הוא בנייה מראש של "ארגז הכלים".

מאחר שמשבר סייבר אינו סוגיה טכנולוגית גרידא, ארגז הכלים שם דגש לא רק על משאבים טכנולוגיים, אלא גם על המרכיב האנושי ושיפור מיומנויותיו ועל הטמעת ידע. כל אלה הם "מכפילי כוח" בעבור הארגון. בכמה מהמרכיבים נעשה שימוש גם בשגרה (לדוגמה: הטמעת מערכות טכנולוגיות והדרכה ותרגול), ואחרים מופעלים רק לקראת התרחשות משבר, או בזמן התרחשותו בפועל (לדוגמה: ביצוע פעולות במערכות הממוחשבות והפעלת צוות לניהול משבר).

כל ארגון אחראי על הכנת ארגז כלים משלו, לנוכח הערכת הסיכונים שביצע, איום ותרחיש הייחוס כלפיו בסייבר[23] ובהתחשב בצרכיו ובמשאביו. הרכבו של ארגז הכלים ייקבע גם בעקבות היעדים ורמות השירות שנקבעו במשרדי הממשלה, המתייחסים למימוש חלקם באחריות המדינתית להבטחת קיומם התקין של יעדי השירות הלאומיים[24]. מכאן, הרגולטורים חשובים מאוד בהגדרת רמת רציפות התפקוד הנדרשת מהארגונים שבאחריותם, ולאורה יבנו הארגונים את ארגז הכלים, יקצו לו תקציב ייעודי וכן תקציב זמין נוסף לחירום, וישלבו אותו בתוכנית העבודה.

את ארגז הכלים מומלץ לבנות תוך התייחסות לחמישה מכפילי כוח: ידע מקצועי; כוח אדם; טכנולוגיות ואמצעים; הסתייעות בגורמים חיצוניים; הכשרה ותרגול. מאחר שהתפיסה מיועדת גם לארגונים ומוסדות ממלכתיים וגם לארגונים ציבוריים ופרטיים, כל ארגון יכול להיעזר בדוגמאות המפורטות להלן ולייצר לעצמו את ההתאמות הנדרשות.

### 1. ידע מקצועי

א. הטמעת התפיסה המובאת במסמך זה, כמסגרת לשפה משותפת ולהעמקת שיתוף הפעולה והשיח, וככלי לבניית תוכנית סייבר להיערכות ולניהול מצבי משבר. תוכנית זו יכולה להיות פרק בתוכנית החירום הארגונית[25], או מסמך נפרד, ומומלץ שתיכתב בסיוע מקצועי של מערך הסייבר הלאומי ו/או הרגולטור או הגורם המנחה, ותאושר על-ידי הנהלת הארגון. ראוי לתקף ולעדכן את התוכנית אחת לשנה, ולרענן אותה עם העלאת הכוננות.

ב. הטמעת תורת ההגנה בסייבר לארגון (תוה"ג), שפותחה במערך הסייבר הלאומי כדי למזער את סיכוני הסייבר של ארגונים במשק הישראלי. התוה"ג מגדירה מתודה סדורה שבאמצעותה כל ארגון יכול להכיר את הסיכונים הרלוונטיים לו, לגבש מענה הגנתי ולממש תוכנית להפחתת

22 ראה הרחבה בפרק הבא

23 איום הייחוס מבוסס על מודיעין ומגדיר את האיומים המרכזיים והממשיים. תרחיש הייחוס מבוסס הערכה ומגדיר את התסריט האפשרי לפעילות עוינת ואופן מימושה. ארגון יכול להסתייע בגורמים חיצוניים בגיבוש איום ותרחיש הייחוס

24 כפי שהוסבר בסעיף הגדרת נכסי הסייבר החיוניים Top-Down, בפרק "מיפוי נכסי הסייבר החיוניים"

25 BCP: Business Continuity Plan (תוכנית להמשכיות עסקית)

הסיכונים בהתאם. את התוה"ג וכן הרחבות מקצועיות בתחום הגנת הסייבר אפשר למצוא באתר האינטרנט של מערך הסייבר הלאומי[26].

ג. הסתייעות בתורות, נהלים ושיטות עבודה מומלצות (Best Practices) בסייבר לארגון, שנכתבו על-ידי מערך הסייבר הלאומי, רגולטור רלוונטי או גורם מנחה מקובל בעולם (למשל מכוני תקנים), בדגש על היערכות וניהול מצבי משבר[27].

### 2. כוח אדם

הגורם האנושי הוא חלק אינטגרלי בהיערכות ובניהול משבר סייבר, ולמצבי משבר יש השפעה על מצבת כוח האדם, בגלל הצורך לפעול בעצימות ובהיקפים גדולים יותר מבשגרה, או בעקבות גיוס מילואים והיעדרות עובדים[28]. על כן נדרש להתייחס להפעלת כוח האדם במצבי משבר, להגדיר בעלי תפקיד חיוניים ותחומי אחריות, לבנות תוכנית לגיבוי ולתגבור כוח אדם חיוני בכל דרגי העבודה ולבחון דרכים ושיטות עבודה לתפקוד עם כוח אדם מצומצם.

א. הקמת צוות היערכות וניהול משבר: מכיוון שהנהלת הארגון מחזיקה באחריות הכוללת להיערכות בסייבר למצבי משבר, והיא תנהל את המשבר אם יתממש, מומלץ שבראש הצוות יעמוד מנכ"ל הארגון או סגנו. משבר סייבר אינו עניין טכנולוגי גרידא, ולכן נוסף על מנהל אבטחת המידע והסייבר, רצוי שצוות ההיערכות וניהול המשבר יכלול גורמים בדרגה ניהולית בכירה, שמכירים את תהליכי העבודה בארגון זמן רב ומגיעים מתחומי ידע שונים (למשל סמנכ"ל תפעול, סמנכ"ל כספים, יועץ משפטי, מנהל הרכש והלוגיסטיקה, אחראי דוברות, קצין ביטחון). בזמן שגרה אחראי הצוות להיערכות, ובזמן משבר לניהולו על כל היבטיו: ריכוז תמונת מצב וביצוע הערכת מצב[29], הכרזה על מצב הכוננות ושינוי רמת הכוננות, ביצוע פעולות לנוכח מצב הכוננות, עבודה מול גורמים בתוך הארגון ומחוץ לו, ולבסוף התאוששות, חזרה למצב שגרה והפקת לקחים והטמעתם[30].

ב. הקמת צוות תגובה טכנולוגי (CSIRT)[31]: צוות מקצועי שייעודו מניעה, זיהוי, התמודדות וטיפול באירוע סייבר והתאוששות מנזקיו. צוות זה כולל גורמי אבטחת מידע וסייבר וגורמי IT, והוא יכול להיות מורכב מעובדי הארגון או ממומחי חוץ שבהם הארגון בוחר להסתייע. בעת משבר ידווח ישירות לצוות ההיערכות וניהול המשבר ויעבוד בהתייעצות ובתיאום עם נציגי יחידות אחרות בארגון ומחוץ לו.

ג. הצבות כוח אדם בחירום: על הארגון למפות את מצבת כוח האדם, את יכולותיו ואת כישוריו, ולבנות תמונת פערים בכוח אדם ובמיומנויות שלהן הוא זקוק להמשך רציפות תפקוד גם בזמן משבר. התהליך יסייע לארגון ליצור הצבות כוח אדם בחירום, כלומר שהתפקיד של חלק מהעובדים יהיה שונה בזמן משבר מהתפקיד שהם ממלאים בשגרה, ולסמן מקורות לתגבור (ויסות פנימי או הסתייעות בגורמים חוץ-ארגוניים). לביצוע מיטבי נדרש להכשיר ולתרגל את העובדים לנושא עוד בזמן שגרה.

ד. הגדרת הארגון "מפעל חיוני"[32]: קבלת אישור "מפעל חיוני" מאפשרת בין היתר שני כלים

---

26 כתובת: https://www.gov.il/he/Departments/Policies/cyber_security_methodology_for_organizations

27 להרחבה בנושא תקנים ורגולציה בתחום אבטחת הסייבר: https://www.gov.il/he/Departments/legalInfo/regulation

28 רלוונטי כאשר משבר הסייבר מתחולל בו-זמנית עם משבר במרחב הפיזי

29 להרחבה ראה נספח ב'

30 להרחבה ראה פרק "ניהול משבר סייבר"

31 CERT: Computer Emergency Response Team. נקרא גם Computer Security Incident Response Team

32 מפעל (ארגון) או חלק ממנו, הפועל או שאפשר להפעילו לצורכי הגנת המדינה, ביטחון הציבור ולהספקת שירותים חיוניים למשק, ואשר נדרש להמשיך ולתפקד גם במצבי משבר. הגדרת ארגון "מפעל חיוני" כפופה לאישור ועדה שמינה שר העבודה, הרווחה והשירותים החברתיים.

חשובים להתמודדות עם מצבי משבר בהקשר של כוח אדם: 1) "ריתוק משקי" של עובדים החיוניים להבטחת רציפות התפקוד של הארגון (לדוגמה גורמי אבטחת מידע וסייבר). עובד חייב שירות ביטחון, שאושר לריתוק משקי, יבצע בחירום את עבודתו במסגרת המפעל החיוני שאליו הוא שייך ולא ייקרא לשירות ביטחוני; 2) איתור, הגדרה ואישור "מגויסי חוץ", שהם מי שאינם עובדים בארגון, ונקראים לעבוד בו בזמן משבר כמקור תגבור. חשוב לבסס את יחסי העבודה עם מגויסי החוץ עוד בשגרה[33].

ה. גיבוש עתודת מומחי סייבר: ארגון יכול לגבש עתודת מתנדבים המומחים במגוון תחומים בעולם הסייבר, ואלה יסייעו לארגון בשגרה ובזמן משבר, הן כצוות חשיבה וסיעור מוחות והן למתן פתרונות טכנולוגיים וניהוליים.

### 3. טכנולוגיות ואמצעים

על הארגון להצטייד בטכנולוגיות ובאמצעים שיסייעו לו להעלות את רמת ההגנה בסייבר, לחזק את יכולותיו לזהות תקיפה ולתת לה מענה, לנהל את המשבר ובה בעת לשמר תהליכי רציפות תפקוד והמשכיות עסקית.

א. מערכות: 1. הטמעת טכנולוגיות הגנה (הזדהות, הצפנה, מניעת קוד עוין וכיו"ב); 2. תשתיות תיעוד וניטור פעילויות במערכות לשם זיהוי אירועי סייבר ולטובת תגובה מהירה וצמצום הנזק (לדוגמה: הגדרת פעולות רצויות לשמירה בקובצי ה-LOG והטמעת מערכות SIEM); 3. טכנולוגיות שיטוי, הטעיה וזיהוי וחקירה של תוקפים (לדוגמה "מלכודות דבש" Honeypots ו"ארגז חול" Sandbox); 4. הטמעת מערכות גיבוי מידע ואחזור נתונים לטובת התאוששות מהירה; מערכות לתיעוד ולניהול אירועי משבר ולתחקור בסיומו (יומן מבצעים); 5. בחינת האפשרות לחיבור למערכת "סייברנט" של ה-CERT הלאומי, המאפשרת שיתוף מידע לטובת התמודדות עם איומי סייבר ואירועי סייבר. 6. את כלל המערכות הטכנולוגיות יש לעדכן עדכון שוטף, או לפי הנחיית הרגולטור/הגורם המנחה.

ב. אמצעים פיזיים: הקמת אתר חלופי (DR) מופרד ומרוחק פיזית מהאתר הראשי ועומד ברמת אבטחה גבוהה, באופן שיקטין את הסבירות ששני האתרים ייפגעו בו-זמנית ויאפשר גיבוי ושחזור מידע; הטמעת נהלים ובקרות כניסה למתקנים של הארגון, כדי למנוע חדירה לסביבת הסייבר באמצעים פיזיים.

ג. אמצעים לוגיסטיים: הצטיידות באמצעים לוגיסטיים ומנהלתיים שיסייעו לעבודה בזמן משבר (עבודה מרחוק, כלכלת עובדים, הסעות וכיו"ב); הצטיידות באמצעי מיגון פיזיים הנדרשים בזמן מצבי חירום ממחולל שאינו סייבר; בדיקה תקופתית של כשירות התשתיות והאמצעים.

### 4. הסתייעות בגורמים חיצוניים

יש כיום גורמים מקצועיים רבים שיכולים לסייע בסייבר לארגון, הן במצב שגרה לטובת ההיערכות והן במצבי משבר.

א. המגזר הציבורי: הסתייעות בכלים מקצועיים של מערך הסייבר הלאומי והרגולטורים המנחים את הארגון (לדוגמה: ידע מקצועי, מענה לאירועי סייבר, הכשרות, הדרכות, תרגילים וביקורות ועוד).

ב. המגזר הפרטי: אם ארגון בוחר להסתייע בשירות של חברות פרטיות (לדוגמה: ייעוץ בנושא ניהול סיכונים, מענה לאירועי סייבר וניהול משבר סייבר, ביטוח וכיו"ב), הכרחי שבהסכמי השירות הנחתמים עימן תתווסף התחייבות שהמענה יינתן גם בזמן משבר (SLA). חשוב שהגורם החיצוני שנותן שירות יכיר את תוכנית ההיערכות של הארגון למצבי משבר,

33 הרחבה בנושאים אלה אפשר למצוא בדף רשות כוח האדם לשעת חירום באתר האינטרנט של משרד העבודה, הרווחה והשירותים החברתיים

ובמידת האפשר ישתתף בתרגילים הקשורים בה ויעודכן בעת התרחשות אירוע חריג. נוסף על כך ארגון יכול להסתייע בידע ובכלים המצויים בארגונים מקבילים בעולם[34].

ג. הסכמי שיתוף פעולה: ארגון יכול לפעול ליצירת הסכמים, בכתב או בעל-פה, עם ארגונים רלוונטיים אחרים (לדוגמה מאותו המגזר), לטובת סיוע הדדי ושיתופי פעולה בסייבר בשגרה ובדגש על מצבי משבר.

### 5. הכשרה ותרגול

תוקפים רבים בסייבר מצליחים להתגבר על אמצעי ההגנה באמצעות שימוש בהנדסה חברתית (Social Engineering). כך הם מנצלים את הגורם האנושי, למשל דרך דיוג (Phishing), שבו התוקף מתחזה לגורם אחר. כאשר מתרחשים אירועי סייבר, הגורם האנושי הוא מרכיב אינטגרלי במתן המענה. על כן להכשרה ולתרגול יש חשיבות רבה בהיערכות בסייבר למצבי משבר ולהעלאת חוסנו של הארגון.

א. הכשרות והדרכות: יינתנו לבעלי תפקידים בארגון, הן בנושאים כלליים לטובת העלאת המודעות ויצירת תרבות ארגונית לאיום הסייבר, והן בנושאים מוגדרים לטובת בנייה ושמירת כשירות. זאת כדי שהעובדים יבצעו את תפקידם בצורה מיטבית בשגרה ובחירום (בדגש על עובדים שמבצעים בחירום תפקיד שונה מהתפקיד שהם מבצעים בשגרה, בהתאם להצבות החירום). בדרג ההנהלה חשוב לכלול הכשרות והדרכות לחיזוק מיומנויות רכות, דוגמת יכולת קבלת החלטות, עבודת צוות והתנהלות תקשורתית.

ב. תרגילים וביקורות: יכולים להיות בהיקפים שונים (רמת פרט, כלל הארגון, מגזר שלם) ובשיטות שונות (תרגיל שולחני, אופרטיבי, סימולטור; ביקורת גלויה/סמויה, מבדקי חדירות). על התרגילים והביקורות להיות חלק מתוכנית העבודה השנתית, להקיף מספר רב ככל שניתן של בעלי תפקידים, כולל רמת ההנהלה וצוות ניהול המשבר, ולהתבצע בשיתוף גורמי חוץ שעימם יש לארגון ממשקים. נדרש שהתרגילים והביקורות יאתגרו ויביאו לידי ביטוי את תוכנית הסייבר להיערכות ולניהול מצבי משבר של הארגון, והמסקנות שיעלו בעקבותיהם ישמשו להפקת לקחים ולעדכונים נדרשים בתוכנית.

במסגרת ארגז הכלים, מצורף בפרק הנספחים שאלון שנועד לשמש ככלי עבודה ומטרתו להעריך את מידת היערכותו של הארגון למצבי משבר בסייבר ולהציע תובנות הנוגעות לנושאים שנדרש לשפר (ראה נספח ג').


## היערכות למצבי משבר ארגז הכלים

34 לדוגמה המרכז לשיתוף ולניתוח מידע של FS-ISAC שחברים בו ארגונים פיננסיים גלובליים

# ניהול משבר סייבר

### 1. "מחזור החיים" של משבר סייבר

לכל משבר סייבר יש "מחזור חיים" ייחודי לו. יש משברים "מתפרצים" אשר מתרחשים בפתאומיות והשלכותיהם ניכרות מייד, ואילו משברים אחרים נבנים בהדרגה (אולם גם אם מסתמנת הסלמה הדרגתית ייתכן שבהמשך תגיע התפרצות). המידע הראשוני יכול להגיע מכמה מקורות: מערכות ניטור ובקרה, סימנים מעידים בנתונים או במידע עסקי, דיווח מגורם פנימי, או עדכון של גורם חיצוני (דוגמת מערך הסייבר הלאומי או רגולטור/גורם מנחה). לנוכח המהירות הרבה שבה משבר סייבר יכול להתפרץ והסיכון בהתרחבותו לארגונים ולמגזרים נוספים, על כל גורם המאתר חשד לאירוע סייבר, או מקבל דיווח בנושא, לעדכן מיידית את כלל הגורמים הרלוונטיים בארגון ומחוץ לו.

את מחזור החיים של משבר סייבר, כתהליך שבו כמה שלבים, ניתן לשרטט כך:

זיהוי: גילוי כי מדובר בהתרחשות חריגה מבחינת השפעותיה על נכסי הסייבר החיוניים של הארגון ועל תהליכי הליבה שלו (איום או פגיעה בפועל), וגיבוש מהיר ככל האפשר של דפוס המענה הדרוש.

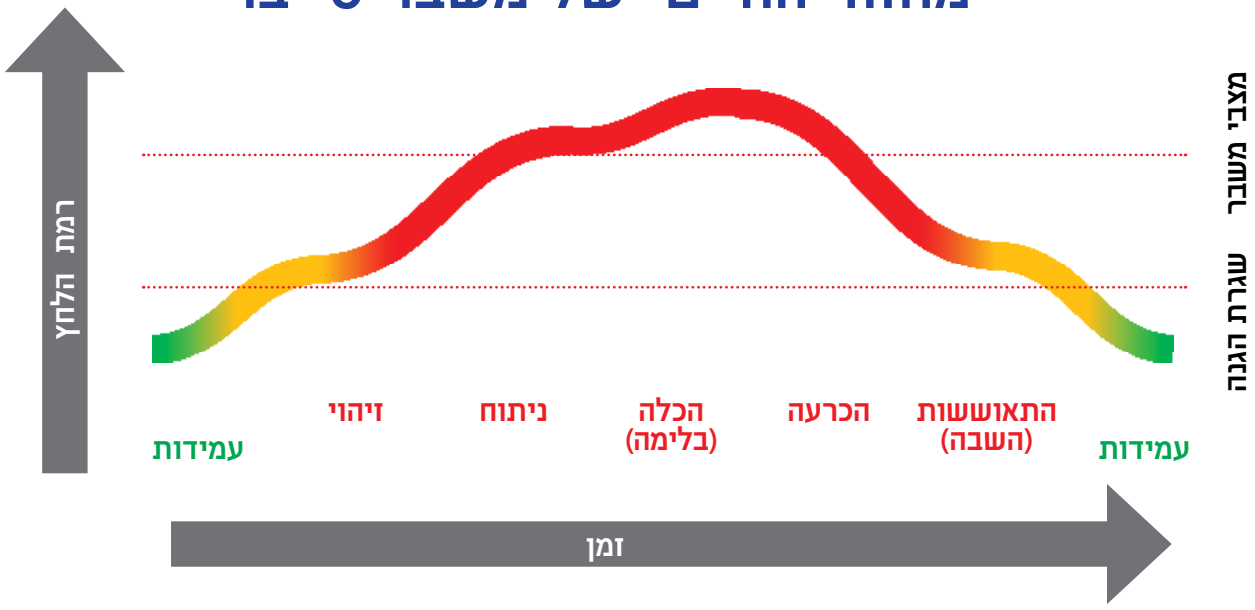
ניתוח: בירור מקיף ומעמיק של אופי ההתרחשות ובדיקה שאין פרצות נוספות, ובחינת השלכותיה על תפקוד הארגון מעבר להיבט הטכנולוגי.

הכלה (בלימה): חסימת התקיפה (השגת שליטה ראשונית) והתרחבותה לנכסי סייבר נוספים, ועצירת החמרת הנזק שהיא גורמת (המשכיות עסקית, תדמית, נזק כלכלי). עבודה לפי תוכנית ניהול משבר הארגונית.

הכרעה: נטרול רכיבי הפגיעה תוך כדי ניסיון לבטל או למזער ככל האפשר את הנזק שכבר נגרם.

התאוששות (השבה): חזרה מבוקרת לפעילות תקינה, הכרזה על סיום המשבר (מצב של שגרת הגנה בסייבר), תחקיר והפקת לקחים, והגדרת צעדים ליישומם.[35]

## "מחזור החיים" של משבר סייבר




35 התרשים לקוח מהאתר של ENISA, סוכנות של האיחוד האירופי לביטחון רשתות ומידע.

### 2. תפיסת הניהול של משבר סייבר: צוות ניהול המשבר

אפשר למנות כמה יעדים (תכליות) מרכזיים בניהול משבר סייבר:

למזער את הפגיעה התפקודית, העסקית-כלכלית והתדמיתית; לשמור על נכסי הסייבר החיוניים ועל נכסי מידע רגיש; להמשיך ולספק שירותים מיטביים גם בעת משבר, בדגש על שירותים חיוניים; לחזק את אמונם של בעלי עניין על-ידי הוכחת יכולת התמודדות טובה במצבי משבר; לסיים במהירות האפשרית את הטיפול באירועי המשבר, להתאושש ולחזור לשגרה.

נדרש שניהול משבר סייבר יתייחס לאיומים ולאתגרים בשני רבדים:

א. התמודדות עם גורמי המשבר: ההיבטים הטכנולוגיים הקשורים למתקפת הסייבר והשפעתם הישירה על נכסי הסייבר (בהובלת צוות התגובה הטכנולוגי).

ב. התמודדות עם השלכות המשבר: להבדיל מאירוע סייבר, משבר סייבר דורש התייחסות מעבר לגבולות הטכנולוגיים, ויש לו השלכות בהיבט הפנים-ארגוני והחוץ-ארגוני, דוגמת רציפות התפקוד של הארגון, השלכות עסקיות-כלכליות והשלכות תדמיתיות.

ההתמודדות בשני הרבדים הללו מצריכה כלים שונים והיא גם באחריותם של גורמים ארגוניים שונים. עם זאת חשוב מאוד הסנכרון בטיפול בשני הרבדים, שכן יש זיקה ביניהם, ולהחלטות ברובד האחד עשויות להיות השלכות ברובד האחר. על כן, ומפאת השלכותיו החמורות של משבר הסייבר על תדמיתו של הארגון, נכסיו, תפקודו ו/או יכולותיו לממש את יעדיו המרכזיים, על משבר הסייבר להיות מנוהל על-ידי צוות ניהול משבר המורכב מדרג בכיר בהנהלת הארגון[36]. צוות זה מנחה ומכוון את פעילות הגורמים הרלוונטיים האחרים בארגון (בין היתר את צוות התגובה הטכנולוגי), וכן מנהל קשר עם בעלי העניין החיצוניים, שחשיבותם רבה בעת משבר.

## תפיסת הניהול של משבר סייבר


36 כפי שהוסבר בסעיף כוח אדם בפרק "היערכות למצבי משבר".

כשמאגדים יחד את המרכיבים שתוארו לעיל, המתווה הכולל של ניהול משבר סייבר נראה כך:


### 3. פעולות בניהול משבר סייבר

בשלב זה של הפרק יפורטו פעולות לביצוע בניהול משבר סייבר. לנוחות הקורא, הפעולות מחולקות לפי מצבי הכוננות בסייבר. אין זה אומר שהכרזה על מצב כוננות מכתיבה בהכרח מימוש של פעולות ספציפיות, אלא שמצבי הכוננות הם כלי עזר להחלטה על פעולות. על כן במצב כוננות סייבר נתון יבצעו ארגונים פעולות שונות זה מזה, לנוכח הסכנה הנשקפת להם והערכת המצב ובהתחשב בכלים ובמשאבים העומדים לרשותם או בהנחיית הרגולטור[37].

מאחר שהתפיסה מיועדת הן לארגונים ומוסדות ממלכתיים והן לארגונים ציבוריים ופרטיים, כל ארגון יכול להיעזר בדוגמאות המפורטות להלן ולייצר לעצמו את ההתאמות הנדרשות. כפי שהוסבר בפרק הקודם, פעולות שלא יוכנו בעוד מועד לא יתאפשר לממשן בזמן משבר, או יתאפשר לממשן חלקית ולא באופן מיטבי. טרם החלטה על פעולה נדרש להביא בחשבון את השלכותיה האפשריות[38].

להלן פירוט הפעולות האפשריות בכל אחד ממצבי הכוננות בסייבר, בחלוקה לפעולות פנים-ארגוניות וחוץ- ארגוניות[39]:

37 הנחיות הרגולטור/הגורם המנחה צריכות להיות מידתיות, ולהתחשב ביכולות הארגון ומשאביו, ובעלויות הכרוכות בביצוע הפעולות

38 לדוגמה, האופן שהארגון בוחר לדבר אירוע או משבר סייבר, כיצד הוא מתמודד עם נוזקת כופר שמטרתה לסחוט תשלום בתמורה להסרת מגבלת הגישה (Ransomware), השפעות על ארגונים מקבילים ועל בעלי עניין, ביצוע פעולות לסילוק הפוגען באופן גלוי או חסוי לתוקף ועוד

39 חשוב לתעד את הפעולות שננקטו בעת ניהול המשבר, בין היתר לצורך תחקור והפקת לקחים, כפי שיפורט בהמשך הפרק

### 3.1. מצב שגרת הגנה בסייבר

במצב שגרת הגנה בסייבר, פרט לפעולות הנעשות להבטחת שגרת הפעילות באיומי סייבר ולהתמודדות עם אירועי סייבר נקודתיים, נערך הארגון לפעולות שינקוט במצבי משבר. כלומר, הארגון עושה פעילות שוטפת תוך בניית יכולות והעלאת כשירות, ושמירה על גמישות לקראת מעבר למצב כוננות סייבר גבוה יותר, כפי שפורט בפרק הקודם שעסק בארגז הכלים.

### 3.2. מצב כוננות סייבר א'

פעולות אפשריות במצב כוננות סייבר א':

פנים-ארגוני: הגברת עירנות, עדכון כלל הגורמים הרלוונטיים בתוך הארגון בהעלאת הכוננות והגברת זמינות[40]; ויסות ו/או תגבור כוח אדם לריכוז מאמץ; איוש/תגבור מרכז השליטה הארגוני; הערכות מצב שוטפות; עדכון תמונת המצב ומאמץ המודיעין; הכנת הודעות לתקשורת ("נצורות"); רענון תוכנית הסייבר לניהול משבר ווידוא מוכנות למעבר למצב כוננות גבוה יותר; נקיטת פעולות נדרשות במערכות הממוחשבות (לדוגמה: בדיקת תקינות, עדכוני אבטחה, הגברת פעילות הניטור במערכות ההגנה השונות, גיבויים ועוד)[41]; ביצוע פעולות נדרשות הקשורות באבטחה הפיזית (לדוגמה הגברת עירנות לאירועים חריגים בארגון ודיווח מידי, החמרת נוהלי הכניסה לארגון ובדיקת תקינות אמצעי האבטחה ועוד).

חוץ-ארגוני: עדכון הרגולטור/הגורם המנחה, מערך הסייבר הלאומי, שותפים וכלל הגורמים הרלוונטיים במצב הכוננות ובתמונת המצב בסייבר, לצורך שיתוף מידע וידע וקבלת הנחיות והמלצות לפעולה; מתן הנחיות לגורמים שהארגון מנחה; איסוף מידע מגורמים פנימיים וחיצוניים רלוונטיים; עדכון ובדיקת קשר עם נותני שירותים שהארגון קשור עימם.

### 3.3. מצב כוננות סייבר ב'

במצב כוננות סייבר ב' יבוצעו כל הפעולות שביצע הארגון במצב כוננות סייבר א', וכן:

פנים-ארגוני: הפעלה ותגבור צוותים מקצועיים רלוונטיים (לדוגמה צוותי תגובה טכנולוגיים, צוות ניהול משבר); איוש מלא של מרכז השליטה ועבודה לפי שעון פעילות ארגוני; מוכנות להפעלת תוכנית הצבות כוח אדם חירום; פעילות דוברות; ביצוע פעולות נדרשות במערכות הממוחשבות (לדוגמה: הפסקת הכנסת קבצים, הקפאת תצורה ובחינת הצורך בניתוק קישורים לא הכרחיים עם מערכות משיקות, צמצום פעילות למינימום, איתור רכיבים שהותקפו, בידוד הסגמנט שבו זוהתה התקיפה, חסימת התקיפה, בדיקה כי אין פרצות נוספות, תיעוד); חלוקת אמצעי מיגון והעלאת המוכנות למעבר למתקן חלופי ובדיקת המערכות הנמצאות בו (רלוונטי כאשר ההסלמה קשורה במחולל חירום פיזי, ואם קיים); נקיטת פעולות נדרשות הקשורות באבטחה הפיזית (לדוגמה: סריקות עיתיות, עיבוי אבטחה והגבלת כניסת מבקרים רק במקרים דחופים ובליווי); צמצום פעולות שאינן חיוניות.

חוץ-ארגוני: מימוש התקשרויות עם גורמים מקצועיים חיצוניים לקבלת סיוע (לדוגמה חברות אבטחת מידע וסייבר, וניהול משבר); מימוש הסכמים שנחתמו לשיתוף פעולה עם ארגונים מקבילים; מתן התראה להגברת זמינות למגויסי החוץ העומדים לרשות הארגון; הפעלת עתודת מומחים בסייבר.

40 בעדכון גורמי פנים וחוץ באירועי סייבר נדרשת שמירה על חשאיות, לטובת "הגנה שקטה" (פעילות בחתימה נמוכה)
41 להרחבה על פעולות לביצוע במערכות הממוחשבות והמלצות בנושא, ניתן להסתייע ברגולטור/גורם מנחה וכן במערך הסייבר הלאומי דרך יצירת קשר עם ה-CERT הלאומי (9344*)

### 3.4. מצב כוננות סייבר ג'

במצב כוננות סייבר ג' יבוצעו הפעולות שנקט הארגון במצב כוננות סייבר ב', וכן:

פנים-ארגוני: הפעלת תוכנית הצבות כוח אדם בחירום; הפעלת ריתוק משקי (בארגונים שאושרו כ"מפעל חיוני"); איוש מתקן חלופי; ביצוע פעולות נדרשות במערכות הממוחשבות (לדוגמה ניתוק כלל הקישורים החיצוניים למערכת); ביצוע פעולות נדרשות הקשורות באבטחה הפיזית (לדוגמה איסור כניסת מבקרים).

חוץ-ארגוני: עבודה לפי שעון פעילות לאומי; הפעלת מגויסי חוץ.

## פעולות אפשריות לנוכח כל אחד ממצבי הכוננות (דוגמה)

| מצב כוננות סייבר א' | | מצב כוננות סייבר ב' | | מצב כוננות סייבר ג' | |
|---|---|---|---|---|---|
| עדכון כלל הגורמים הרלוונטיים | ויסות ו/או תגבור כוח אדם | הפעלת צוותים מקצועיים פנים ארגוניים | איוש מלא של מרכז השליטה הארגוני | עבודה בהתאם לשעון פעילות לאומי | הפעלת תוכנית הצבות כוח אדם בחירום |
| תגבור מרכז השליטה הארגוני | ביצוע הערכות מצב שוטפות | עבודה לפי שעון פעילות | מוכנות להפעלת תוכנית הצבות כוח אדם בחירום | הפעלת ריתוק משקי | הפעלת מגויסי חוץ |
| עדכון תמונת מצב ומאמץ המודיעין | הכנת הודעות "נצורות" לתקשורת | פעילות דוברות | מיגון ולוגיסטיקה | איוש מתקן חלופי | מיגון ולוגיסטיקה |
| רענון ועבודה לפי תוכנית ההיערכות בסייבר למשברים | וידוא מוכנות למעבר למצב כוננות גבוה יותר | מימוש התקשרויות עם נותני שירותים | מימוש הסכמי שיתוף פעולה עם ארגונים מקבילים | ביצוע פעולות במערכות הממוחשבות | ביצוע פעולות להגברת האבטחה הפיזית |
| ביצוע פעולות במערכות הממוחשבות | ביצוע פעולות להגברת האבטחה הפיזית | ביצוע פעולות במערכות הממוחשבות | ביצוע פעולות להגברת האבטחה הפיזית | | |

### 3.5. התאוששות: חזרה למצב שגרת הגנה בסייבר

על חזרה למצב שגרת הגנה בסייבר יכריז מנכ"ל הארגון, או בעל התפקיד שהסמיך לכך (למשל ראש צוות ניהול המשבר). עם ההכרזה על חזרה למצב של שגרת הגנה בסייבר[42] יש לעדכן את כל הגורמים הרלוונטיים בתוך הארגון ומחוץ לו. על הארגון להגדיר יעדי התאוששות[43], להעריך את הנזקים שנגרמו ולפעול לצמצמם, ולהפיק לקחים מהתנהלותו במשבר בהקדם, כדי לשפר את איכות המענה העתידי למצבי משבר. חשוב לדון בין היתר בנושאים האלה:

א. סקירה כרונולוגית של האירועים והפעולות שבוצעו, החל בהחלטה על העלאת הכוננות בסייבר וכלה בחזרה לשגרת הגנה.

ב. הערכת התנהלות הארגון ויעילות הפעולות שננקטו בתגובה לאירועים בכלל התחומים (טכנולוגי, ניהולי, לוגיסטי, דוברות ועוד), כולל נושא ההסתייעות ושיתוף הפעולה עם גורמים חיצוניים.

ג. הערכת יעילות ההכנות שבוצעו בשגרה ("ארגז הכלים").

ד. זיהוי נושאים לשיפור ולשימור והערכת צרכים עתידיים. גיבוש לקחים, הטמעתם והפצתם לבעלי העניין בתוך הארגון ומחוץ לו.

ה. תיקוף תוכנית ההיערכות בסייבר למצבי משבר.

42 בהתאם לעקרונות להורדת רמת הכוננות, כפי שפורטו בפרק "מצבי הכוננות בסייבר ועקרונות לשינוי רמת הכוננות".
43 לדוגמה: חזרה לפעילות עסקית מלאה בפרק זמן מסוים

# נספחים

## נספח א':
## שאלון למיפוי נכסי הסייבר החיוניים

1. כחלק מהיערכות לשמירה על רציפות התפקוד המשקית בזמן חירום, הוגדרו במשרדי הממשלה יעדי השירות ורמות שירות. את התהליך מובילה רשות חירום לאומית (רח"ל) בשיתוף משרדי הממשלה.

2. כחלק מתהליך המיפוי חשוב לזהות נכסי סייבר (מערכות מחשוב, תשתיות, מערכות תקשורת, שרתים, בקרים וכו') התומכים בתהליכי הליבה, על מנת לקבל תמונה רחבה ומעמיקה בנושא ולהגדירם נכסי סייבר חיוניים שנדרשים ברמה גבוהה של הגנה בסייבר.

3. לביצוע המיפוי, להלן שאלון קצר המסתמך על יעדי השירות שהוגדרו במשרדכם, ונועד להצביע על נכסי סייבר חיוניים אשר פגיעה בהם תגרום נזק ארוך וממושך.

4. את התהליך נכון וכדאי לבצע בשיתוף המנחים ממרכז מגזרים של מערך הסייבר הלאומי, וכן עם יחידות הסייבר המגזריות או עם הרגולטור הרלוונטי.

| מס' משימה | יעדים משרדיים | האם יעד השירות מחייב עבודה עם מערכות מחשוב? | אם כן, מהי/מהן המערכת/ות התומכ/ות ביעד השירות? | מהו פרק הזמן שיעד השירות יכול להמשיך לתפקד ללא מערכות מחשוב? | האם יש יכולת לחזור לשגרת עבודה על-ידי מערכות חלופיות? | האם תיפגע רמת השירות עקב זליגת/ גניבת מידע ממערכות מחשוב? | האם תיפגע רמת השירות עקב השבתת מערכות מחשוב? | האם תיפגע רמת השירות עקב שיבוש נתונים במערכת מחשוב? |
|---|---|---|---|---|---|---|---|---|
| 1 | נא לפרט | לא/ כן בתלות מעטה עד בינונית/<br>כן בתלות רבה | נא לפרט | לא יכול/<br>יכול עד שבוע/<br>יכול יותר משבוע | לא/כן, תוך 12 שעות/<br>כן, תוך 24-12 שעות/<br>כן, תוך 3-1 יממות/<br>כן, יותר מ-3 יממות | אין פגיעה/<br>פגיעה קלה עד בינונית/<br>פגיעה חמורה | אין פגיעה/<br>פגיעה קלה עד בינונית/<br>פגיעה חמורה | אין פגיעה/<br>פגיעה קלה עד בינונית/<br>פגיעה חמורה |
| 2 | | | | | | | | |
| 3 | | | | | | | | |


RANSOM!
Your files have been encrypted

# נספח ב':
# הערכת מצב סייבר

תכלית הערכת המצב בסייבר היא לסייע בפיתוח הבנת המשמעות של המתרחש על בסיס מידע ועובדות וחשיבה משותפת, ולאחר מכן הגדרת פעולות לביצוע. הערכת המצב תהיה בראשות הדמות הבכירה בארגון, או מי שהסמיך לכך, במועד שנקבע מראש (למשל אחת לשבוע) או לנוכח הנסיבות, בהשתתפות דרג ניהולי בכיר (בדרך כלל צוות היערכות וניהול משבר) וגורמי מקצוע רלוונטיים אחרים. על הדיון עצמו להיות תמציתי ותכליתי.

פורמט דיון הערכת מצב אמור להיות קבוע, תוך התאמות נדרשות למאפייני המצב. חלקו הראשון מורכב מהצגת תמונת המצב של כל המידע הכמותי והאיכותי הרלוונטי, הידוע בזמן נתון על המתרחש במרחב הסייבר ובמרחב הפיזי, והשלכותיו על הארגון. על מנת לייעל את הדיון, תמונת המצב צריכה להיות מתואמת עם הגורמים השונים לפני ביצועה, והיא כוללת שני רבדים:

א. תמונת מצב טכנולוגית: יעדי התקיפה ומועדיה, גורמי התקיפה ככל שידועים, נכסי סייבר שנפגעו (בדגש על נכסי סייבר חיוניים), השפעות על תהליכי ליבה ושירותים, סטטוס ההתמודדות עם התקיפה, קשר עם גורמים חיצוניים מקצועיים.

ב. תמונת מצב לגבי היבטי המעטפת: לרבות השלכות על רציפות התפקוד והמשכיות עסקית, השלכות עסקיות-כלכליות, היבטי תקשורת ודוברות, היבטים משפטיים ועוד.

## תמונת מצב סייבר (דוגמה)

**נכון ל:**_____

| נושא הדיווח | תמונת המצב (בתמצית) | פעולות שננקטו / מתוכננות |
|---|---|---|
| מועד התקיפה | | |
| הגורם התוקף | | |
| סוג המתקפה | | |
| נכסי סייבר שנפגעו | | |
| מטרות ודרישות התוקפים | | |
| מידע ונתונים שזלגו | | |
| שירותים/תהליכים שנפגעו | | |
| פרסום ופומביות | | |
| ממשקים עם גורמים מחוץ לארגון | | |
| היבטי מעטפת | | |

בחלקו השני של הדיון, אל מול תמונת המצב, ייבחנו המשמעויות והחלופות ויתקבלו החלטות והמלצות לפעולה. לאחר מכן ייכתב סיכום של ההחלטות שהתקבלו ויופץ לגורמים הרלוונטיים, בדגש על משימות לביצוע.

## סוגיות לדיון בהערכת מצב (לדוגמה)

| | | | |
|---|---|---|---|
| היכולת להתמודד עם האירוע | סיוע מקצועי נדרש (ספקים/יועצים/ מומחים) | פעולות נדרשות מול גורמים חיצוניים, בדגש על רגולטור/ גורם מנחה | פעולות נדרשות מול לקוחות |
| סדרי עדיפויות לאישוש תהליכי ליבה ושירותים | החלטות לגבי פעולות במערכות הממוחשבות (בדגש על נכסי סייבר חיוניים) | החלטות לגבי פעולות הקשורות באבטחה הפיזית | משמעויות בהקשר היבטי כוח אדם |
| עדכון עובדים | הנחיות בהיבטי אבטחת מידע וביטחון | תקשורת ודוברות כלפי חוץ | היבטים משפטיים |
| **פעולות לביצוע** | | | |

לסיכום:

# דיון הערכת מצב

עקרונות

- תמציתי ותכליתי
- פורמט הדיון וההצגות בו מוגדרים מראש
- דגש על שינויים שאירעו מאז הדיון הקודם

שלבים

1

**עדכון והבהרת משמעויות (פורמט קבוע מראש)**

1. הצגת תמונת מצב טכנולוגית: ראש צוות ה- CSIRT / מנהל חדר מצב
2. השלמות בתחומים עיקריים: מנהלים מקצועיים רלוונטיים, דוברות, ייעוץ משפטי

על מנת לייעל את דיוני הערכת המצב, תמונת המצב צריכה להיות מתואמת עם הגורמים השונים **לפני** דיון הערכת המצב

2

**קבלת החלטות**

1. הצגת ההחלטות הנדרשות בנושאים העומדים על הפרק, והחלופות העיקריות
2. דיון על החלופות
3. קבלת החלטות על דרכי הפעולה

3

- סיכום מהיר בכתב של ההחלטות שהתקבלו
- הפצת הסיכום והמשימות לגורמים הרלוונטיים

# נספח ג': שאלון מידת היערכות למצבי משבר בסייבר (TOP 10)

השאלון להלן מבוסס על התפיסה המובאת במסמך זה, והוא כלי עבודה להנהלת הארגון לבחינת מידת ההיערכות הארגונית למצבי משבר בסייבר[44]. תוצאות השאלון מאפשרות לדרג את היערכות הארגון וללמד מהן הפעולות שעליו לעשות כדי לשפר את היערכותו.

אפשר להשתמש בשאלון כפי שהוא, או לבצע בו התאמות, כל ארגון ברמתו, ומומלץ שיבוצע על-ידי הגורמים האחראים בארגון לרציפות תפקוד וההגנה בסייבר, לניהול סיכונים ולהיערכות לחירום. אפשרות נוספת היא להסתייע בגורם חיצוני אובייקטיבי שיבצע את תהליך הבחינה. בהתאם לאופי הארגון מומלץ להגדיר פרק זמן לביצוע הבחינה (בממוצע אחת לשנה), ובעקבותיה לבנות תוכנית לשיפור.

השאלון מתבסס על רשימת נושאים ראשיים, ובהם חלוקה לנושאי משנה. על מנת להקל את מילוי התשובות ולאפשר צפייה נוחה בתשובות המתקבלות (כולל בצורה גרפית), אפשר לבנות את השאלון ב-Excel או בכלי אחר. הסבר על אופן חישוב הציון נמצא בסוף השאלון.

**רשימת הנושאים בשאלון:**

**אחריות ארגונית [10% מהציון הכולל של הסקר]**

**השאלות להלן עוסקות בהגדרות האחריות הארגונית למצב משבר בסייבר.**

1. האם הוגדרו בארגונך בעלי תפקידים ותחומי אחריותם **להיערכות בעת שגרה**, לקראת מצב משבר בסייבר?
   א. כן, בדרגים מקצועיים ובדרגי הנהלה [3.34%]
   ב. כן, בדרג מקצועי בלבד [1.66%]
   ג. כן, בדרג הנהלה בלבד [1.66%]
   ד. לא הוגדרו [0%]
2. האם הוגדרו בארגונך בעלי תפקידים ותחומי אחריותם **בעת התרחשות משבר סייבר** (פגיעה אפשרית בנכס סייבר הנובעת מפעילות מכוונת)?
   א. כן, בדרגים מקצועיים ודרגי הנהלה [3.34%]
   ב. כן, בדרג מקצועי בלבד [1.66%]
   ג. כן, בדרג הנהלה בלבד [1.66%]
   ד. לא הוגדרו [0%]

44 את השאלון ניתן למצוא באתר האינטרנט של מערך הסייבר הלאומי, בכתובת: https://survey.gov.il/he/preparedness_for_cyber_crises

3. האם הוגדרו "**תהליכי ליבה**" בארגונך (תהליכים שמבצע ארגון על מנת לממש את יעדיו המרכזיים ו/או יעדים שהוגדרו לו על ידי הרגולטור)?

א. הוגדרו תהליכי ליבה באופן מלא [3.34%]

ב. הוגדרו תהליכי ליבה באופן נקודתי / חלקי [1.66%]

ג. לא הוגדרו כלל תהליכי ליבה [0%]

### נכסי סייבר חיוניים [10%]

**השאלות להלן עוסקות בנכסי סייבר החיוניים לארגון שלך. נכס סייבר חיוני הוא מערכת תקשוב (לרבות חומרה ותוכנה), המשמשת בין היתר לאחסון, ניהול, עיבוד והעברה של מידע, ו/או לתפעול שליטה ובקרה, אשר תפקודה התקין נדרש לשם רציפותו של תהליך ליבה.**

4. האם הוגדרו **נכסי סייבר החיוניים** לארגונך (על-ידי הארגון או על-ידי הרגולטור)?

א. הוגדרו נכסי הסייבר החיוניים באופן מלא [5%]

ב. הוגדרו נכסי הסייבר החיוניים באופן נקודתי / חלקי [2.5%]

ג. לא הוגדרו כלל נכסי הסייבר החיוניים [0%]

5. האם מבוצעות בארגונך בדיקות של **ספקים ונותני שירות**, לצורך זיהוי איומים וסיכונים על נכסי סייבר חיוניים ממערכות/שירותי הספקים?

א. מבוצעות באופן מלא, כולל תיקופן מעת לעת [5%]

ב. מבוצעות באופן נקודתי / חלקי (רק בעת תחילת עבודה עם ספק חדש, או רק בעבור חלק מהספקים) [2.5%]

ג. לא מבוצעות כלל [0%]

### ניהול סיכונים [10% + 5% בונוס]

**השאלות להלן עוסקות בתהליכי ניהול סיכונים בסייבר המבוצעים בארגונך (איתור סיכונים בסייבר והערכת החומרה וההשלכות הנובעות מהתממשות סיכונים אלו).**

6. באיזו תדירות מבוצע תהליך של ניהול סיכונים בסייבר בארגונך?

א. מבוצע לפחות פעם בשנה [5%]

ב. מבוצע פעם ב-2-3 שנים [3.3%]

ג. מבוצע פחות מפעם ב-3 שנים [1.6%]

ד. לא מבוצע כלל [0%]

7. שאלת בונוס: במידה שמבוצעים תהליכי ניהול סיכונים בסייבר (סעיפים א'-ג' בשאלה 6), באיזו מידה מיושמות ההמלצות של תהליכי ניהול הסיכונים?

א. מיושמות במידה רבה מאוד [5%]

ב. מיושמות במידה רבה [3.75%]

ג. מיושמות במידה בינונית [2.5%]

ד. מיושמות במידה מועטה [1.25%]

ה. לא מיושמות כלל [0%]

8. באיזו מידה ארגונך נערך לפי תרחישי ייחוס לתקיפה עוינת בסייבר (תסריטים לפעילות נגד הארגון ואופן מימושם)?

א. במידה רבה מאוד [5%]

ב. במידה רבה [3.75%]

ג. במידה בינונית [2.5%]

ד. במידה מועטה [1.25%]

ה. כלל לא [0%]

### מצבי כוננות בסייבר [10% + 5% בונוס]

**השאלות להלן עוסקות במצבי כוננות סייבר בארגונך. מצבי כוננות סייבר הינם "מדרגות" המשקפות את מידת הדריכות וההיערכות הנדרשת. לדוגמה: "שגרת הגנה"= ללא נזק לנכסי סייבר; "כוננות סייבר א'"=איום ממשי לפגיעה בנכס סייבר חיוני; "כוננות סייבר ב'"=פגיעה בנכס/י סייבר חיוני/ים וכן הלאה.**

9. האם מוגדרים בארגונך מצבי כוננות בסייבר?

א. מוגדרים באופן מלא [10%]

ב. מוגדרים באופן חלקי/נקודתי [5%]

ג. לא מוגדרים כלל [0%]

10. שאלת בונוס: במידה שמוגדרים מצבי כוננות סייבר (סעיפים א'-ב' בשאלה 9), האם הוגדרו הסמכויות הניהוליות להכרזה ו/או לעדכון מצבי הכוננות?

א. הוגדרו באופן מלא [2.5%]

ב. הוגדרו באופן חלקי/נקודתי [1.25%]

ג. לא הוגדרו [0%]

11. שאלת בונוס: במידה שמוגדרים מצבי כוננות סייבר (סעיפים א'-ב' בשאלה 9), האם הוגדרו הפעולות הנדרשות לביצוע בכל מצב כוננות?

א. הוגדרו באופן מלא [2.5%]

ב. הוגדרו באופן חלקי/נקודתי [1.25%]

ג. לא הוגדרו [0%]

### ידע מקצועי [10%]

12. האם ארגונך עושה שימוש ב"תפיסה הלאומית להיערכות ולניהול מצבי משבר בסייבר" (המסמך להלן)?

    א. כן [3.33%]

    ב. לא [0%]

13. האם ארגונך עושה שימוש בתורת הגנה בסייבר (כגון מסמך ה"תוה"ג" שהופץ על-ידי מערך הסייבר הלאומי, או בתו"ל ייעודי אחר)?

    א. כן [3.33%]

    ב. לא [0%]

14. באיזו מידה ארגונך עושה שימוש בתקנים ושיטות עבודה מומלצות ("Best Practices") מטעם ארגון רשמי, כגון תקני ISO, GDPR,NIST, תקנות הגנת הפרטיות?

    א. במידה רבה מאוד [3.33%]

    ב. במידה רבה [2.5%]

    ג. במידה בינונית [1.66%]

    ד. במידה מועטה [0.83%]

    ה. כלל לא [0%]

### כוח אדם [10%]

**השאלות להלן עוסקות בכוח אדם לטיפול במשבר סייבר, בדרג ההנהלה ובדרג המקצועי.**

15. אם ארגונך מוגדר "משק לשעת חירום" או "מפעל חיוני", האם בוצע "ריתוק משקי" של עובדים אשר חיוניים להבטחת רציפות התפקוד שלו (המשכיות עסקית)?

    א. כן, באופן מלא [3.33%]

    ב. כן, באופן חלקי/נקודתי [1.66%]

    ג. לא בוצע [0%]

    ד. לא רלוונטי (הארגון אינו מוגדר משק לשעת חירום/מפעל חיוני) [השמט שאלה וחשב דירוג סעיף על סמך שאלות 16-17 בלבד]

16. האם הוגדר בארגונך **צוות ייעודי** בדרג ההנהלה לצורך היערכות וניהול משבר סייבר?

    א. כן [3.33%] [אם ארגונך אינו מוגדר "משק לשעת חירום" או "מפעל חיוני" סכום לפי: 5%]

    ב. לא [0%]

17. האם הוגדר בארגונך צוות תגובה בדרג המקצועי-טכנולוגי (Incidence Response Team) למתן מענה במקרה של משבר סייבר (יכול להיות צוות תגובה פנימי או במיקור חוץ)?

א. כן [3.33%] [אם ארגונך אינו מוגדר "משק לשעת חירום" או "מפעל חיוני" סכום לפי: 5%]

ב. לא [0%]

### טכנולוגיות ואמצעים [10%]

**השאלות להלן עוסקות בטכנולוגיות ואמצעים המוטמעים בארגונך להעלאת רמת ההגנה בסייבר ולמתן מענה לתקיפות.**

18. באיזו תדירות מבוצע גיבוי של נתונים?

א. רציפה או יומית [2.5%]

ב. שבועית [1.66%]

ג. חודשית ומעלה [0.825%]

ד. כלל לא מבוצע גיבוי [0%]

19. האם לארגונך יש טכנולוגיות לתיעוד וניטור פעולות במערכותיו הממוחשבות?

א. כן [2.5%]

ב. לא [0%]

20. האם לארגונך יש אתר DR (התאוששות מאסון) מופרד ומרוחק באופן פיזי מהאתר הראשי (לטובת גיבוי מערכות, מידע, והמשכיות עסקית)?

א. כן [2.5%]

ב. לא [0%]

21. באיזו מידה ארגונך ערוך ברמה הלוגיסטית לתמוך בכוח האדם הדרוש לטיפול במשבר סייבר (לדוגמה עבודה מרחוק, כלכלת עובדים, הסעות, וכיו"ב)?

א. במידה רבה מאוד [2.5%]

ב. במידה רבה [1.875%]

ג. במידה בינונית [1.25%]

ד. במידה מועטה [0.625%]

ה. כלל לא [0%]

### הסתייעות בגורמים חיצוניים [10%]

**השאלות להלן עוסקות בהסתמכות על גורמים חיצוניים, לצורך היערכות וטיפול במשבר סייבר.**

האם ארגונך מסתייע בכלים ובידע מקצועי של מערך הסייבר הלאומי, רגולטורים, או בשירותים של חברות פרטיות לצורך:

22. מתן מענה לאירועי סייבר? כן [2.5%] / לא [0%]
23. הכשרות והדרכות כוח אדם? כן [2.5%] / לא [0%]
24. תרגול הארגון? כן [2.5%] / לא [0%]
25. ביצוע ביקורות? כן [2.5%] / לא [0%]

### הכשרה ותרגול [10% + 6% בונוס]

26. האם מבוצעות הכשרות והדרכות לבעלי תפקידים בארגונך (עובדים והנהלה), בנושאי סייבר (לדוגמה העלאת מודעות ויצירת תרבות ארגונית)?
    א. כן, באופן תדיר (כולל רענונים) [3.33%]
    ב. כן, באופן מזדמן / נקודתי בלבד (לדוגמה, בעת קליטת עובדים בלבד) [1.66%]
    ג. לא מבוצעות [0%]
27. באיזו תדירות מבוצעים בארגונך תרגילי סייבר?
    א. מבוצעים לפחות פעם בשנה [3.33%]
    ב. מבוצעים אחת ל-2-3 שנים [2.22%]
    ג. מבוצעים פחות מפעם ב-3 שנים [1.11%]
    ד. כלל לא מבוצעים [0%]
28. שאלת בונוס: אם מבוצעים תרגילי סייבר (סעיפים א'-ג' בשאלה 27), האם דרג ההנהלה משתתף בתרגילים אלו? כן [2%] / לא [0%]
29. שאלת בונוס: אם מבוצעים תרגילי סייבר (סעיפים א'-ג' בשאלה 27), האם דרגים מקצועיים-טכנולוגיים משתתפים בתרגילים אלו? כן [2%] / לא [0%]
30. שאלת בונוס: אם מבוצעים תרגילי סייבר (סעיפים א'-ג' בשאלה 27), האם גורמי חוץ (ספקים) משתתפים בתרגילים אלו? כן [2%] / לא [0%]
31. באיזו תדירות מבוצעות בארגונך ביקורות (פנימיות או חיצוניות), בנושא סייבר?
    א. מבוצעות לפחות פעם בשנה [3.33%]
    ב. מבוצעות פעם ב-2-3 שנים [2.22%]
    ג. פחות מפעם ב-3 שנים [1.11%]
    ד. לא מבוצעות כלל [0%]

### ניהול משברי סייבר [10%]

32. האם לארגונך יש תוכנית כתובה (נוהל) לניהול משברי סייבר?

א. כן [3.33%]

ב. לא [0%]

33. האם הוגדרו בארגונך אנשי קשר לדיווח במקרה של התפתחות משבר סייבר (מיהם האנשים שעמם יוצרים קשר בתוך הארגון ומחוץ לו - רגולטור, שותפים, לקוחות, ואיך ליצור את הקשר)?

א. כן [3.33%]

ב. לא [0%]

34. האם מוגדרות בארגונך פעולות לחזרה לשגרה והפקת לקחים בעת התאוששות ממשבר סייבר (אופן גיבוש לקחים והטמעתם)?

א. כן [3.33%]

ב. לא [0%]

### אופן חישוב הציון

**הציון המרבי בשאלון הינו 100% + 16% "בונוס".**

**החישוב בכל חלק מתבצע על ידי סכימה של מספר הנקודות (לכל סעיף מצויין ה-% שהוא מקנה).**

**הערה: בסעיף "כוח אדם", יש שאלה לגבי "משק לשעת חירום" ו"מפעל חיוני" (שאלה 15) עם תשובה אפשרית של "לא רלוונטי". אם ארגונך אינו מוגדר "משק לשעת חירום" או "מפעל חיוני", יש לבצע סכימה לפי שתי השאלות הנותרות (16+17 בלבד), והניקוד המרבי לכל אחת מהן הוא 5%. אם ארגונך כן מוגדר "משק לשעת חירום" או "מפעל חיוני", תבוצע סכימה של סך הנקודות עבור כל שלוש השאלות בסעיף (15-17), וכל שאלה מקבלת ניקוד מרבי של 3.33%.**

**כדי לקבל את הציון הכללי לשאלון, סוכמים את כלל האחוזים, על פני כלל הסעיפים.**

## חישוב לדוגמה בעבור סעיף מצבי כוננות בסייבר (שאלות 9-11 בשאלון)

**סעיף "מצבי כוננות בסייבר" מקנה לכל היותר [10%] + 5% בונוס]. לכן בעבור הבחירות המתוארות מטה (מסומנות בצהוב), יקנה הסעיף 7.5% בחישוב הכולל (5% + 1.25% + 1.25%)**

9. האם מוגדרים בארגונך מצבי כוננות בסייבר?

א. מוגדרים באופן מלא [10%]

ב. מוגדרים באופן חלקי/נקודתי [5%]

ג. לא מוגדרים כלל [0%]

10. שאלת בונוס: במידה שמוגדרים מצבי כוננות בסייבר (סעיפים א'-ב' בשאלה 9), האם הוגדרו הסמכויות הניהוליות להכרזה ו/או לעדכון מצבי הכוננות?

א. הוגדרו באופן מלא [2.5%]

ב. הוגדרו באופן חלקי/נקודתי [1.25%]

ג. לא הוגדרו [0%]

11. שאלת בונוס: במידה שמוגדרים מצבי כוננות בסייבר (סעיפים א'-ב' בשאלה 9), האם הוגדרו הפעולות הנדרשות לביצוע בכל מצב כוננות?

א. הוגדרו באופן מלא [2.5%]

ב. הוגדרו באופן חלקי/נקודתי [1.25%]

ג. לא הוגדרו [0%]

סייבר ישראל
משרד ראש הממשלה
מערך הסייבר הלאומי

לפנ


*9344
preparedness@cyber.gov.il
www.cyber.gov.il

חפשו אותנו