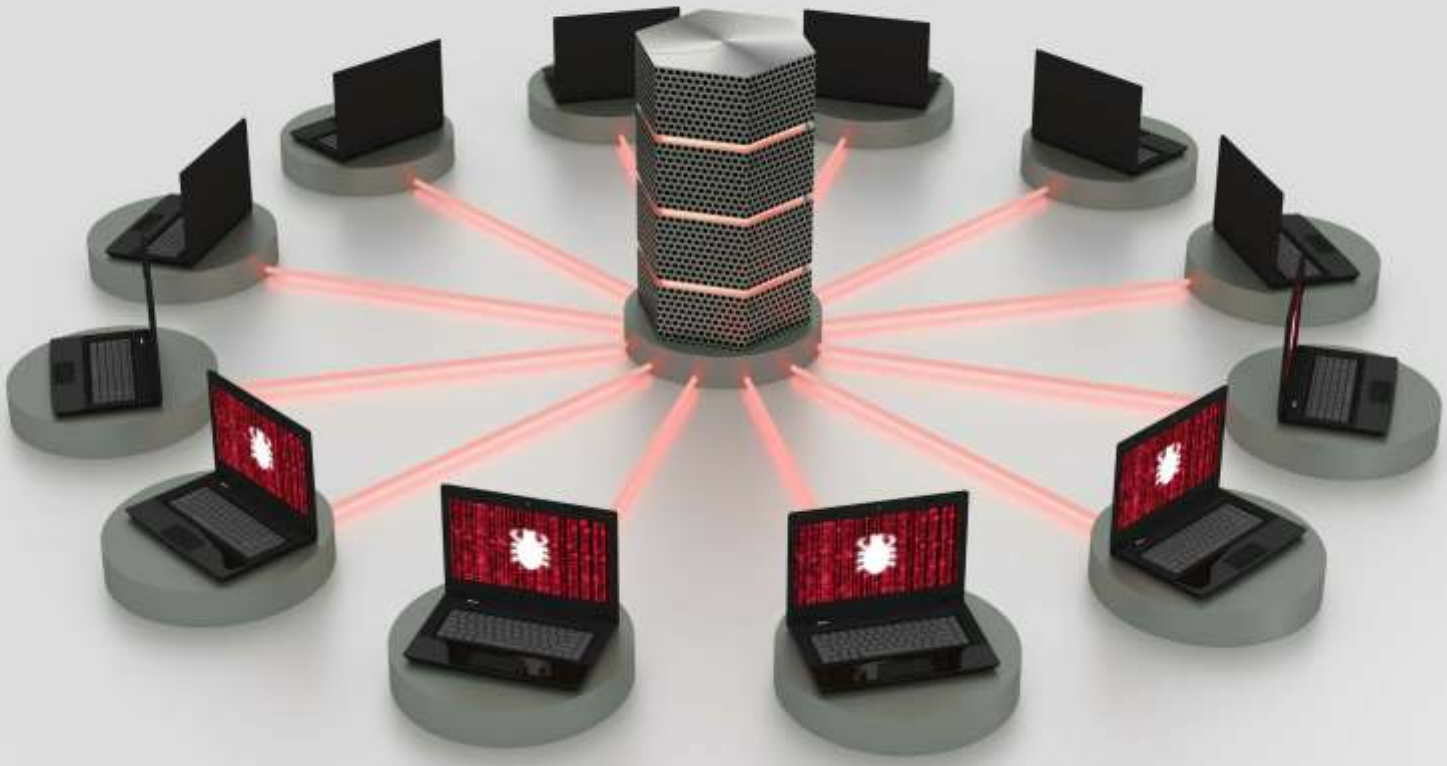
סייבר ישראל
מערך הסייבר הלאומי

המלצות ליישום (Best Practices)
היערכות כנגד תקיפות מניעת שירות מבוזרות (DDoS)



סייבר ישראל
מערך הסייבר הלאומי

המלצות ליישום
(Best Practices)

היערכות כנגד תקיפות מניעת שירות מבוזרות (DDoS)

נובמבר
2020

תוכן עניינים

1. מבוא (Introduction) 3
2. מטרות ויעדים (Goals & Objectives) 7
3. קהל היעד (Target Audience) 7
4. תיחום המסמך (Scope of This Document) 7
5. איומים הנגזרים מתקיפת מניעת שירות מבוזרת (DDoS) 7
6. המלצות ליישום - היערכות כנגד תקיפות מניעת שירות מבוזרות 11
7. נספחים (Appendixes) 27
8. קיצורי שמות (Acronyms) 36
9. מסמכים ישימים (Applicable Documents) 39

היערכות כנגד תקיפות מניעת שירות מבוזרות (DDoS)

1. מבוא (Introduction)

1.1 כללי

אחד האיומים מול מערכות ותשתיות החשופות לאינטרנט הינו תקיפות מניעת שירות מבוזרות (DDoS).
כתוצאה מכך, פעילות עסקית של ארגונים אשר הותקפו שובשה עד לכדי קיומה של השבתה מלאה וממושכת, דבר אשר גרם לארגונים נזקים מהותיים.
בהמשך למגמה זו, ניתן להניח כי התדירות והמורכבות הטכנית של תקיפות אלו רק תגבר בעתיד הקרוב, דבר המחייב את ארגונים במשק הישראלי להיערך בהתאם.

1.2 הבדלים עקרוניים בין תקיפת מניעת שירות, לתקיפת מניעת שירות מבוזרת

תקיפת מניעת שירות מהווה שם מתכלל לשורה של תקיפות אשר מטרתן העיקרית היא להשבית או לשבש פעילות של נכס סייבר/תהליך עסקי, וזאת ע"י יצירת עומס חריג על משאביו. במקרה זה, הגורם היוזם את תקיפה זו הינו נכס סייבר יחיד אשר נשלט ע"י תוקף. פעמים רבות הארגון המותקף יכול לחסום את כתובת ה-IP של נכס הסייבר התוקף, ולפיכך ההשפעה העסקית של תקיפה זו היא בד"כ נמוכה.
תקיפת מניעת שירות מבוזרת מציגה מתווה פעולה דומה, אך במקרה זה התוקף שולט על מספר נכסי סייבר הפועלים באופן מתואם כנגד היעד (דוגמת ביצוע מספר גלי תקיפה אשר מקורם מנכסי סייבר הממוקמים במקומות שונים ברחבי העולם). כפועל יוצא מכך, נפחי התקיפה גבוהים משמעותית, וביצוע פעולות הגנה מקובלות, דוגמת חסימת כתובות ה-IP של נכסי הסייבר התוקפים, אינן אפקטיביות דיים.

1.3 עקרונות ההגנה

עקרונות ההגנה להיערכות בפני תקיפות מניעת שירות מבוזרות מתבססות על אבני הבניין הבאים; אנשים, תהליכים וטכנולוגיה (People, Process, Technology).

א. **אנשים** - הארגון נדרש לוודא כי ההון האנושי אשר ברשותו, וברשות ספקים רלוונטיים בשרשרת האספקה (דוגמת ספק שירותי האינטרנט), מסוגל לספק מענה אפקטיבי כנגד תקיפות סייבר מקובלות, דוגמת תקיפות מניעת שירות מבוזרות. בכלל זה, ישנה חשיבות למעורבות ארכיטקט הגנה בסייבר בשלב גיבוש הפתרון ובחינת האפקטיביות שלו. כמו כן, עולה הצורך כי הארגון יוודא כי ברשותו צוות תגובה לאירועי סייבר, לצד צוות ניטור הפעיל 24/7, וזאת במטרה כי במקרה של חשד לאירוע או אירוע אמת, הוא מסוגל יהיה לגלותו, לזהותו ולסכלו תוך צמצום ההשלכות הנגזרות על הפעילות העסקית.

ב. **תהליכים** - הארגון נדרש לוודא כי תהליכים תומכים מותאמים לספק מענה הולם להתמודדות עם תקיפות מניעת שירות מבוזרות.

ניתן לחלק את התהליכים בהתאם לקטגוריות הבאות:

1. תהליכים לבניין הכוח, אשר כוללים בין השאר ניהול סיכונים, איסוף וניתוח מודיעין איומים סייבר, הכשרות מקצועיות, בדיקת מוכנות וכשירות (דוגמת בדיקות חוסן ותרגילים), עדכון תרחישי התקיפה ומענים בתוכנית המשכיות עסקית של הארגון (BCP) וספר מרשם (Playbook), וקיומם של נוהלי עבודה רלוונטיים. כמו כן, תהליך פיתוח מאובטח[1] נדרש לכלול התייחסות לעיצוב לאבטחה (Secure by Design), אבטחה כברירת מחדל (Secure by Default) תוך אימוץ ארכיטקטורה מאובטחת, ובכלל זה וידוא כי התשתית מאפשרת הקצאה של משאבים בהתאם לצורך (Auto Scaling), וקיומה של יכולת שרידות והתאוששות מאסון תוך צמצום למינימום את הצורך במעורבות יד-אדם.

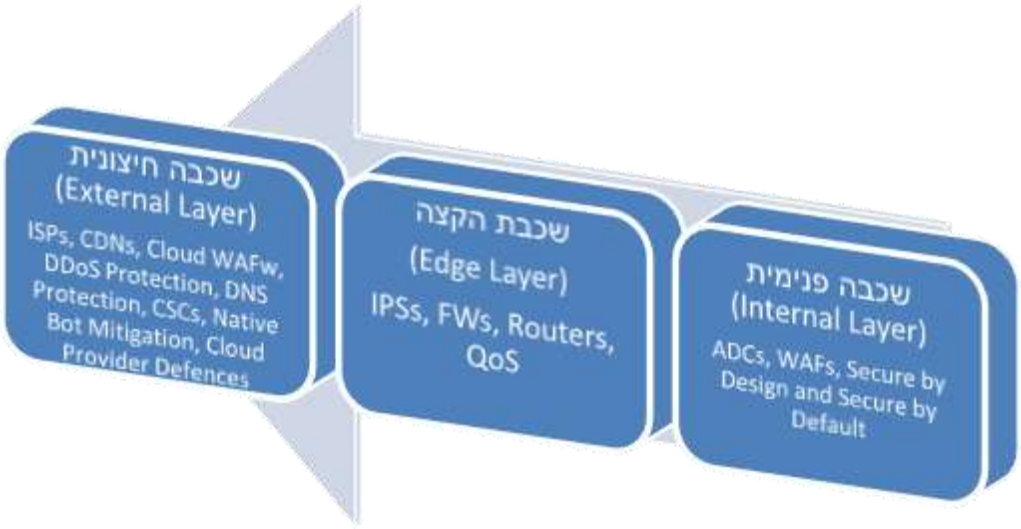
2. תהליכים להתמודדות עם התקיפה, אשר כוללים בין השאר גילוי וזיהוי של התקיפה, וביצוע פעולות הגנה בהתאם לספר מרשם (Playbook) ונוהלי עבודה רלוונטיים.

3. תהליכים לבחינת איכות מענה הפתרון, וזאת תוך בחינה עיתית של היצע הפתרונות בשוק ביחס לצורכי הארגון.

ג. **טכנולוגיה** - הארגון נדרש לוודא כי ארכיטקטורת ההגנה הטכנולוגית מותאמת לספק מענה בפני תקיפות מניעת שירות מבוזרות.

מקובל לחלק את ארכיטקטורה זו בהתאם לשלוש שכבות הגנה.

[1] פיתוח מאובטח - עבודת מנהל הגנת סייבר CISO עם גופי הפיתוח בארגון
https://www.gov.il/he/departments/general/securedevelopment



תרשים 1: שכבות ארכיטקטורת ההגנה מפני תקיפות למניעת שירות מבוזרות (DDoS)

להלן סקירה של כל שכבת הגנה בהתאם לתפקידה:

מס'	שם שכבת ההגנה	תפקיד השכבה
.1	שכבה פנימית (Internal Layer)	שכבה זו אחראית לספק הגנה ישירה על נכסי הסייבר הנמצאים ברשות הארגון (דוגמת אתר Web). בכלל זה, שכבה זו כוללת התייחסות לבנייה נכונה של ארכיטקטורת מערכות ורשתות תוך מימוש עקרונות מקובלים, דוגמת עיצוב לאבטחה (Secure by Design) ואבטחה כברירת מחדל (Secure by Default).
.2	שכבה הקצה (Edge Layer)	שכבה זו אחראית לספק הגנה על קישוריות הארגון לאינטרנט. מקובל כי שכבה זו כוללת שימוש בפתרונות הגנה מסורתיים, ושילוב יכולות ההגנה של ספק האינטרנט (ISP).
.3	שכבה חיצונית (External	שכבה זו כוללת שימוש בגורמי צד-שלישי לשם ביזור תשתית וביצוע פעולות הגנה מתקדמות, לרבות ספק שירותי האינטרנט (ISP). שכיח כיום כי המימוש בפועל מבוסס על רכישה של פתרון הגנה במודל של שירות

	Layer)	כתוכנה (SaaS), ולא הטמעה עצמאית של פתרון מסוג זה. מקובל כי את אמצעי האבטחה הקיימים בשכבה זו ניתן להפעיל באופן קבוע או בהתאם לצורך.

טבלה 1: שכבות ההגנה בפני תקיפות מניעת שירות מבוזרת (DDoS)

ראוי לציין כי לאור מורכבות ההגנה בפני תקיפות מניעת שירות מבוזרות, מומלץ כי ארגונים יאמצו את עקרון הגנה לעומק (Defense in Depth), וזאת תוך שימוש בכל שכבות ההגנה.

ראוי לציין כי קיום שכבות ההגנה בפועל תלוי בארכיטקטורה וסביבת פעולה. כך לדוגמא, בעת עבודה עם ספק שירותי ענן ציבוריים, הספק עשוי להציע ללקוחותיו שירותי הגנה מובנים, כך שהגבולות בין שכבת הקצה, לשכבה החיצונית, עשוי להיות מטושטש.

יש לוודא כי מערך האבטחה הינו בעל תאימות לפרוטוקולים חדשים הנעשה בהם שימוש במרחב הסייבר, דוגמת HTTP /2 ו-HTTP /3 ו-DoH.

הפרמטר המהותי לבחינת רמת האפקטיביות של מערך האבטחה הינו "הזמן האפקטיבי לביצוע אִפְחוּת (Mitigation)".
להלן נוסחה מקובלת לחישוב פרמטר זה:
"הזמן האפקטיבי לביצוע אִפְחוּת" = הזמן הנדרש לגילוי וזיהוי תקיפה + הזמן הנדרש לביצוע פעולות אִפְחוּת אפקטיביות.
ובאנגלית:

Effective Time to Mitigation (TTM) = Time to Detect Attack + Time to Apply Effective Mitigation

חישוב "הזמן האפקטיבי לביצוע אִפְחוּת" מחייב הכרה מעמיקה של התהליכים העסקיים, יחסי התלות, מאפיינים טכניים שונים של נכסי הסייבר, אופי השימוש בנכסי הסייבר (דוגמת מספר לקוחות פעילים בזמן נתון), וביצוע בדיקות אמפיריות לשם תיקוף.

2. מטרות ויעדים (Goals & Objectives)

מסמך זה מציג המלצות ליישום לשם התמודדות עם תקיפות מניעת שירות מבוזרות (DDoS).

3. קהל היעד (Target Audience)

מסמך זה נכתב עבור מנהל הגנת הסייבר בארגון (CISO), מוסמך מתודולוגיות הגנת סייבר, מוסמך מיישם הגנת סייבר, מוסמך טכנולוגיות הגנת סייבר (ארכיטקט הגנה בסייבר), אנשי תקשורת נתונים/תקשוב/IT וסיסטם.
גורמים נוספים אשר עשויים להפיק ערך מוסף ממסמך זה הם מנהל מערכות המידע (CIO - Chief Information Officer) וגורמים עסקיים הנדרשים לאשר את הערכת הסיכונים של נכס הסייבר / התהליך העסקי.

4. תיחום המסמך (Scope of This Document)

המסמך "היערכות כנגד תקיפות מניעת שירות מבוזרות (DDoS)" מתמקד בהמלצות ליישום לשם היערכות כנגד תקיפות מניעת שירות מבוזרות אשר מתמקדות בקישור של תשתית הארגון לרשת האינטרנט.
ראוי לציין כי המסמך אינו כולל הרחבה בנושאים שלגביהם מערך הסייבר הלאומי כתב ופרסם מסמכים ייעודיים. דוגמה לנושא מסוג זה הינה הגנה פרטנית על מערכת ותשתית, דבר הזוכה למענה במסגרת *'תורת ההגנה בסייבר לארגון'* אשר נכתבה ופורסמה על-ידי מערך הסייבר הלאומי.

5. איומים הנגזרים מתקיפת מניעת שירות מבוזרת (DDoS)

פרק זה סוקר את האיומים העיקריים הנגזרים מתקיפות מניעת שירות מבוזרת (DDoS):

	שם האיום	תיאור
1.	מניעת שירות (DOS - Denial of service)	תוקף עשוי לגרום לשיבוש פעילות עסקית עד לכדי השבתתה למשך זמן ממושך. בכלל זה יש לתת את הדעת כי השפעות עשויות להיות ברמת השירות/הממשק הבודד (דוגמת את מסחר מקוון) או

	שם האיום	תיאור
		מספר רב של שירותים/ממשקים (דוגמת אתר מסחר מקוון וממשק התחברות עובדים מרחוק).
.2	נטישת לקוחות	תוקף אשר הצליח לשבש או להשבית את הפעילות העסקית של שירות מקוון של הארגון, עשוי לגרום לנטישת לקוחות, ומעבר שלהם למתחרה.
.3	פגיעה במוניטין	תוקף אשר הצליח לשבש או להשבית את הפעילות העסקית של שירות מקוון של הארגון, עשוי לגרום לפגיעה בשמו הטוב של הארגון, וחשש של לקוחות פוטנציאליים להצטרף לארגון אשר עשוי להיתפס על ידם כגורם פחות מקצועי/מהימן.
.4	פגיעה במהימנות ושלמות נתונים	תוקף עשוי לשלוח שטף (Burst) פעילויות (Sessions) לנכס סייבר, ולאחר זמן קצר להפסיק את הפעילויות. במקרה של נכסי סייבר העושים שימוש בטרנזקציות (דוגמת שרתי מסד נתונים), הדבר עשוי לפגוע במהימנות ושלמות נתונים. להלן מספר דוגמאות: א. העדר מקום לכתיבת הלוגים בדיסק. ב. "קריסה" של נכס הסייבר עקב העומס החריג. ג. גלגול "קדימה ואחורה" בתדירות גבוהה של לוגים המשרתים את מסד הנתונים, עשוי לגרום לבסוף להשחתה שלהם (Data Corruption), בין אם עקב נעילות (Locks), או עקב סיבה אחרת.
.5	סחיטה	תוקף עשוי לאיים ולממש תקיפת מניעת שירות מבוזרת כנגד הארגון אם תנאי מסוים לא יתקיים (דוגמת תשלום כספי). יצוין כי אם הארגון יענה לדרישות התוקף, ישנה סבירות גבוהה כי הדבר יהווה פתח למעשי סחיטה נוספים.

	שם האיום	תיאור
.6	ניצול לרעה של תשתית הארגון לשם תקיפת צד-שלישי	תוקף עשוי לנצל לרעה את תשתית הארגון לשם תקיפת צד-שלישי. דוגמא שכיחה לכך הינה שימוש בהתקני IoT לא מוגנים לשם מימוש תקיפות מניעת שירות מוגברות (Amplifiers). במקרה דנן, מעבר לפגיעה אפשרית בזמינות, סודיות, מהימנות ושלמות המידע ונכסי הסייבר המעורבים, הדבר עשוי לחשוף את הארגון לעיצומים רגולטורים ותביעות משפטיות מצד הגורמים אשר נפגעו.
.7	הקטנת הזמן הממוצע בין תקלות /(MTBF) פגיעה באמינות נכסי הסייבר	א. יצירת עומס חריג על נכסי הסייבר בארגון עשוי לקצר את אורך החיים שלהם, ולהעלות את התדירות לקיומן של תקלות, דבר אשר עשוי להשבית או לשבש פעילות לאורך זמן של תהליכים עסקיים. ב. עלייה בהוצאה הכלכלית עקב התקלות, דבר אשר עשוי לגרום לקיצוץ תקציב הגנת הסייבר.
.8	גרימת הוצאות כספיות חריגות	לשם שמירה על רמות שירות מצופות, ארגונים עשויים להידרש להוצאות חריגות בגין הצורך לבצע שדרוג או הפעלה חריגה ולא מתוכננת של מערך הגנת הסייבר, נכסי הסייבר, הגדלת רוחב הפס או הגדלת קיבולת נכסי הסייבר. יצוין כי במקרה של ענן ציבורי, תוקף עשוי לנצל לרעה את היכולת המובנית בתשתית הענן להגדלת המשאבים ו/או זמינותם הגבוהה, ולגרום לחיובים חריגים של הארגון ע"י ספק הענן (EDoS - Economic Denial of Sustainability).

	שם האיום	תיאור
.9	מסך עשן	תוקף עשוי להשתמש בתקיפת מניעת שירות מבוזרת כמסך עשן, וזאת במטרה להסתיר מהמגן את קיומה של תקיפה נוספת כנגד הארגון.
.10	עקיפת מנגנון אבטחה באמצעות יצירת עומס חריג	תוקף עשוי ליצור עומס חריג אשר יאפשר ניצול חולשה מובנית באמצעי אבטחה (דוגמת WAF), ובכך הוא יוכל לעקוף מנגנון אבטחה קיים (דוגמת מנגנון לסינון קלט זדוני).

טבלה 2: סקירת איומים עיקריים הנגזרים מתקיפות מניעת שירות מבוזרת (DDoS)

לשם ההמחשה, הטבלה הבאה סוקרת מספר סוגי תקיפות מניעת שירות מבוזרת שכיחות:

מס'	קטגוריה	סוג	דוגמאות למימוש	השלכות
.1	Volumetric	צריכת רוחב פס גבוהה	CLDAP, SSDP, NTP, Memcached	אובדן קישוריות לרשת; אובדן יכולת לבצע העלאה / הורדה
.2	TCP state exhaustion	מיצוי משאבים קיימים	SYN flood, teardrop	איטיות במתן מענה לבקשות לקוחות ע"י השרת או לא העדר יכולת להגיב כלל לבקשות
.3	Application	עומס יתר על שרת אפליקציה	HTTP GET flood, DNS flood	איטיות במתן מענה לבקשות לקוחות ע"י

				האפליקציה או העדר יכולת להגיב כלל לבקשות
4.	Application	עומס יתר על שרת אפליקציה + ניצול לרעה של חולשה קיימת	Slowloris, R.U.D.Y and other HTTP session attacks	איטיות במתן מענה לבקשות לקוחות ע"י האפליקציה או העדר יכולת להגיב כלל לבקשות
5.	Application	עומס יתר על תהליכי ניהול לוגיקה עסקית (Business Logic)	Shopping cart excessive item addition\reduction	איטיות במתן מענה לבקשות לקוחות ע"י האפליקציה, פגיעה בביצועים או העדר יכולת להגיב כלל לבקשות

טבלה 3: סקירה של תקיפות מניעת שירות מבוזרת שכיחות (DDoS)

6. המלצות ליישום - היערכות כנגד תקיפות מניעת שירות מבוזרות

פרק זה מציג רשימה של המלצות ליישום, אשר מימוש נכון שלהן יסייע בהיערכות כנגד תקיפות מניעת שירות מבוזרות (DDoS):

מס'	ההמלצה
המלצות כלליות	

מס'	ההמלצה
1.	מומלץ כי הארגון יגדיר לכל תהליך עסקי/נכס סייבר מדדים מקובלים, וזאת בהתאם לצרכים העסקיים שלו. יש לוודא כי המדדים הוחלו בהתאם לצורך בנכסי הסייבר השונים. להלן מספר דוגמאות למדדים מקובלים: א. רוחב הפס (Bandwidth) -מדד לכמות הנתונים שניתן להעביר ממקור ליעד, במשך זמן נתון, על גבי רשת נתונים. יחידת מידה בסיסית - ביט (סיבית) לשנייה - Bits per second (bps). ב. רוחב פס יעיל/תפוקה (Throughput) - מדד לכמות הנתונים הממשית, העוברת בנתיב נתון, בפרק זמן מוגבל, בהתחשב באילוצים הבאים: 1) גודל המידע המועבר. 2) איכות ביצועי התקני הרשת. 3) הזמן בו מועבר המידע. התפוקה קטנה או שווה לרוחב הפס: Throughput=<Bandwidth ג. מספר פקטות מידע/מנות בזמן נתון. יחידת המדידה הבסיסית - Packets per second (pps). ד. מספר בקשות HTTP\S (או פרוטוקול רלוונטי אחר) בזמן נתון. יחידת המדידה הבסיסית - Request per second (rps). ה. השהיה (Delay) - מסגרת הזמן הנדרשת למנה/פקטת מידע (Packet) להגיע מקצה לקצה. יחידת מידה בסיסית - שניות. ו. שיהוי (Latency) - מסגרת הזמן הנדרשת למנה/פקטת מידע (Packet) להגיע מקצה לקצה, וחזרה. שם חילופי זמן הלוך-ושוב (RTT - Round Trip Time). יחידת מידה בסיסית - שניות.

מס'	ההמלצה
	ז. רְצוּד (Jitter) - עיכוב זמן לא סדיר בשליחת מנות/פקטות מידע ברשת. יחידת מידה בסיסית - אחוזים. לעיתים נעשה שימוש גם בשניות.[2] ח. אובדן מנות/פקטות מידע (Packet Loss) - אובדן מנות נמדד כאחוז (Percent's) מהמנות שאבדו, ביחס לחבילות שנשלחו. ט. גודל המנה המקסימלי (MTU) - המנה/פקטת המידע הגדולה ביותר הניתנת להעברה כיחידה אחת ברשת, וזאת ללא צורך בביצוע פעולת קיטוע (Fragmentation). יחידת המדידה הבסיסית - בתים (bytes). י. מספר קישורים (Connections) בזמן נתון. יחידת המדידה הבסיסית - Connections per second. יא. אורך חיים לפעילות משתמש (Session Timeout). יחידת המדידה הבסיסית - שניות. יב. אורך חיים לבדיקת חיות TCP (TCP keepalive). יחידת המדידה הבסיסית - שניות. יג. הזמן האפקטיבי לביצוע אִפְחוּת (Effective TTM). יחידת המדידה הבסיסית - שניות. יד. מדדים מקובלים מעולם המשכיות העסקית (דוגמת RTO, RPO).
2.	מומלץ כי הארגון יבצע באופן עתי מיפוי של טווח כתובות ה-IPv4\IPv6, ה-FQDN's וה-AS's אשר ברשות הארגון, וזאת תוך התייחסות למיקום הלוגי והפיזי של נכסי הסייבר והתהליכים. בכלל זה, יש לבצע תשאול לגורמי התפעול השונים, ספק האינטרנט וכן לבצע חיפוש יזום במאגרי מידע ציבוריים מקובלים. יצוין כי ניתן לראות מקרים בהם יש ברשות הארגון ציוד (דוגמת HVAC) אשר הפגיעה בו עשויה לגרור השבתה רוחבית, אך הארגון אינו ער לכך כי ציוד זה מקושר לאינטרנט.

[2] נוסח חילופי: רְצוּד (Jitter) - רְצוּד מוגדר כשינויי התזמון של קצות אות מהערכים המקוריים שלהם. הסטייה יכולה להיות במונחים של מופע, זמן או רוחב פס האות, ערך זה נמדד באחוזים.

מס'	ההמלצה
.3	מומלץ כי הארגון יבצע סקר סיכונים (Risk Assessment) לניתוח השפעות אפשריות על הפעילות העסקית במקרה של תקיפת מניעת שירות מבוזרת. יש לתת את הדעת להשלכות אפשריות על פעילות מול ספקי הארגון, דוגמת ספק ענן ציבורי או ספק חיצוני המתחזק את אתר האינטרנט של הארגון. כמו כן, יש לתת את הדעת לאיומים רלוונטיים וזאת תוך התייחסות למימדים מקובלים, דוגמת: עצימות (250 GB/s, TBps 4 וכו'), סוג (בהתאם לעיל) וזמן (דקות, שעות, ימים, שבועות וכד').
.4	מומלץ כי הארגון יעשה שימוש במודיעין איומים בסייבר (Cyber Threat Intelligence) לשם הכרת שיטות התקיפה העדכניות, ופיתוח תוכנית תגובה בהתאם. בכלל זה מומלץ לעקוב אחר אירועי סייבר אשר התרחשו בארגונים בעולם, בדגש על ארגונים במגזר הפעילות הבינלאומי והמקומי, וזאת תוך בחינת עצימות, סוג, משך התקיפה, נכסי סייבר שהושפעו מהתקיפה, מניע וזהות התוקף (ככל שניתן לזהותם ברמת ודאות סבירה), תדירות התקיפות, סקירת פגיעויות אשר נוצלו לרעה במסגרת התקיפה, רמת אפקטיביות אמצעי האבטחה אשר נעשה בהם שימוש ע"י הצד המגן, השלכות נגזרות (דוגמת זמן השבתה/שיבוש פעילות עסקית, האם נגרם נזק משני דוגמת השפעה על ערך מנייה או קיומה של נטישת לקוחות ומעבר למתחרה, תביעות לקוחות וגורמי צד-שלישי), הפקת לקחים והמלצות ליישום לשם שיפור המוכנות והכשירות לאירועים דומים.
המלצות לאבטחת השכבה הפנימית (Internal Layer)	
.5	מומלץ כי הארגון יוודא כי תשתית התקשוב והמערכות תוכננו בהתאם לעקרון עיצוב לאבטחה (Secure by Design). להלן מספר דוגמאות:

מס'	ההמלצה
	א. קיומו של מצב אל-כשל (fail-safe), וזאת ע"י שימוש ביתירות (Redundancy) או דרך חלופית. יש לוודא שמצב זה מתקיים מקצה לקצה (End to End). ב. קיומו של מצב התאוששות אוטונומי במקרה של כשל (Self- Healing). ניתן לממש זאת בצורה אפקטיבית בעת שימוש בארכיטקטורת Micro-Services. ג. מעבר לתצורת עבודה Stateless. ד. אימוץ עקרונות הנדסת כאוס (Chaos Security). ה. יכולת הגדלה/הקטנה של קיבולת באופן דינמי (Auto Scaling). ו. הגדרת ספים (Thresholds) ורפים (Bars) המעידים על קיומה של פעילות תקינה, ופעילות חריגה/חשודה, לרבות החלת API Throttling. ז. שימוש ב-CDN לאחסון תוכן סטטי/דינמי. יש לוודא ביזור למספר אתרים בלתי תלויים ברחבי העולם. ח. בעת עבודה עם ענן ציבורי, יש לבחון את המלצות הספק לבנייה של ארכיטקטורה נכונה. ט. קיומה של יכולת אפקטיבית לביצוע דילוג לעבודה מלאה בענן ציבורי או דילוג לעבודה בספק ענן ציבורי אחר או דילוג לעבודה באתר צל (Shadow Site) בספק אחר.
6.	מומלץ כי הארגון יעשה שימוש בחומרה התומכת בתקנים מקובלים להתמודדות עם עומסים בתקשורת נתונים. דוגמא ליישום: א. IEEE 802.1Qbb Priority Flow Control (PFC) ב. IEEE 802.3x Flow control with Pause frames

מס'	ההמלצה
7.	מומלץ כי הארגון יעשה שימוש במערכות ניהול עומסים באפליקציות (ADC - Application Delivery Controller). יש לוודא כי הפתרון הנבחר כולל את היכולות הבאות: א. מתן מענה 3-7 OSI layers. ב. הורדת עומסים בעת עבודה עם תעבורה מוצפנת (Offloading). ג. הורדת עומסים בעת עבודה עם תכנים (Content) ותעבורת TCP. ד. בדיקת חיות (Liveness) של האפליקציה, וזאת ע"י ביצוע סימולציה של פעולות מקובלות של משתמש טיפוסי. ה. ניתוב מבוסס נתיב (Path-based routing) - העברה של בקשת לקוח ליעד על סמך URL ספציפי. ו. ניתוב מבוסס נכס סייבר (Host-based routing) - העברה של בקשת לקוח ליעד על סמך HTTP header ספציפי. ז. מתן מענה ייחודי לבקשת לקוח (Custom HTTP response) ח. ניתוב מבוסס שדות - העברת בקשה ליעד על סמך standard and custom HTTP headers and methods, query parameters, and source IP addresses. ט. תמיכה בפרוטוקול ICAP. י. תמיכה בשיטות מקובלות לניהול התמדה בפעילות (Persistence Session).
8.	מומלץ כי הארגון יעשה שימוש בחומת אש אפליקטיבית (WAF - Web Application Firewall) ו/או RASP. יש לוודא כי הפתרון הנבחר כולל את היכולות הבאות: א. מנגנון Anti-Bot מובנה. יש לתת דגש להשלמת יכולות ב-HTTPS\HTTP שאינם קיימים בד"כ ב-IPSs.

מס'	ההמלצה
	ב. מנגנון Anti-Fraud מובנה. ג. חסימת תקיפות לפי חתימות סטאטיות המתעדכנות מספר פעמים ביום, וזאת על סמך מודיעין איומים סייבר. ד. תמיכה בפאצ'ים וירטואליים (Virtual Patches). ה. גילוי ואיתור איומים בתווך מוצפן. ו. יכולת בידול בין פעילות משתמש אנושי, לפעילות מכונה. בכלל זה, יש לוודא תמיכה במנגנונים מקובלים לאתגור (Challenge) המשתמש. דוגמא ליישום: שימוש ב-CAPTCHA, ביומטריה התנהגותית (Behavioral Biometrics) או שימוש בחידות מתמטיות/פאזלים (Puzzles) שעל צד הלקוח לפתור. ז. חסימת תקיפות בהתאם לחריגה מפרופיל התנהגות טיפוסי של משתמש. לרבות, שילוב יכולות לגילוי זיהוי אנומליה (Anomaly Detection) וחריג חשוד כטעות (Outlier). ח. SDK המאפשר שילוב באפליקציית מובייל יכולת לבחון בזמן אמת את מצב ההיגיינה הטכנולוגית של נכס הסייבר בעת גישה מרחוק. ט. מיסוך זהות נכסי הסייבר ושירותי המערכת (Masking). לדוגמא: החלפת ערכי ברירת מחדל של HTTP Headers X-ASPNET-VERSION, X-Powered-By , בערכים חלופיים. י. יכולת בניית חתימה חדשה לתקיפה ללא צורך במעורבות יד-אדם, וללא הסתמכות על שירות מודיעין איומים בסייבר (Cyber Threat Intelligence). דוגמא ליישום: בניית חתימה על סמך גילוי וזיהוי דפוסים ייחודים החורגים מ-Baseline מאושר או באמצעות דרך אחרת. יא. מתן גישה בהתאם למודל "גישה מבוססת סיכון מסתגל" (RAdAC - Risk Adaptive-Based Access Control); על פי גישה זו, מתבצעת הרחבה למודל גישה מבוססת תכונה (ABAC), כך שהרשאות המשתמש

מס'	ההמלצה
	נקבעות בזמן הריצה בהתאם לתכונות שונות ותוך התחשבות ברמת הסיכון. לדוגמא: 1) שילוב מודיעין איומים בסייבר במערך האבטחה, לרבות שימוש במזהים (IOAs\IOCs) לחסימת תקיפות ופעילות חשודה [דוגמת חסימת גישה מכתובת IP בעלת רמת אמון נמוכה (מוניטין נמוך) עקב שיוך לתשתית קמפיין תקיפה מוכרת או שרת פרוקסי אנונימי]. 2) הגדרת רשימות שחורות (Blacklist) ורשימות לבנות (Whitelist) של כתובות IP בודדות וטווחי כתובות (מקור/יעד), פורטים, שירותים, חלון זמנים, ספקי אינטרנט, מיקום גיאוגרפי (Geofencing\GEO Location)[3], וכד'. 3) אימוץ עקרונות מקובלים לאימות רציף (Continuous Authentication) ואימות מסתגל (Adaptive Authentication). יב. ביצוע Device Profiling.
9.	מומלץ כי הארגון יעשה שימוש בפתרון מקובל לחסימת הורדה והרצה של נוזקה (Malware) בנכסי הסייבר, וזאת לשם סיכול האפשרות לגיוסם לטובת ביצוע תקיפות מניעת שירות מבוזרות בזמן אמת או בעתיד.
10.	מומלץ כי הארגון יטייב באופן עתי תוכן קבצים מקובלים אשר מטרתם להגדיר למנועי חיפוש אילו דפים יש/אין לבצע להם אינדקס (Index). דוגמא לקבצים מקובלים: א. robots.txt ב. Sitemap

[3] לאור העובדה כי מיפוי כתובות ה-IP ביחס למיקום הגיאוגרפי אינו תמיד עדכני/מדויק, יתכנו מצבים שבהם יעשה שימוש בכתובות IP על-ידי גורמים מחוץ למדינת ישראל, למרות שהרישום יעיד כי כתובות אלו משויכות למדינת ישראל.

מס'	ההמלצה
	המלצות לאבטחת שכבת הקצה (Edge Layer)
.11	מומלץ כי הארגון יבצע הפרדה פיזית/לוגית בין ערוצי השירותים, וזאת לשם צמצום ההשפעה של תקיפת מניעת שירות על כלל הערוצים השונים (ניהול המשאבים בערוץ נפרד). להלן מספר דוגמאות: א. הפרדה בין ערוץ ההתחברות מרחוק (VPN), לערוץ המשרת אתר מסחר מקוון. ב. הפרדה בין ערוץ גלישה באינטרנט, לערוץ B2B. ג. הפרדה בין ערוץ דוא"ל, לערוץ המשרת אתר מסחר מקוון. ד. הפרדה בין ערוץ גלישה באינטרנט, לערוץ המשרת תשתית VoIP.
.12	מומלץ כי הארגון יעשה שימוש מערכת למניעת חדירות (IPS - Intrusion Prevention System). יש לוודא כי הפתרון הנבחר כולל את היכולות הבאות: א. מנגנון Anti-Bot מובנה. ב. חסימת פעולות התחזות (Spoofing). ג. חסימת תקיפות לפי חתימות סטאטיות המתעדכנות מספר פעמים ביום, וזאת על סמך מודיעין איומים בסייבר. ד. תמיכה בפאצ'ים וירטואליים (Virtual Patches). ה. גילוי ואיתור איומים בתווך מוצפן. ו. יכולת בידול בין פעילות משתמש אנושי, לפעילות מכונה. בכלל זה, יש לוודא תמיכה במנגנונים מקובלים לאתגור (Challenge) המשתמש.

מס'	ההמלצה
	ז. חסימת תקיפות בהתאם לחריגה מפרופיל התנהגות טיפוסי של משתמש. לרבות, שילוב יכולות לגילוי זיהוי אנומליה וחריג חשוד כטעות. ח. חסימת פעילות אופיינית לסריקת פורטים (דוגמת TCP SYN scan, TCP connect scan, UDP port scan, SCTP INIT scan). ט. תמיכה ביכולת העברת תעבורה חשודה/זדונית לבולען (Sinkhole) ול"חור שחור" (Blackholing). י. מתן גישה בהתאם למודל "גישה מבוססת סיכון מסתגל". ראו לעיל. א. האטה יזומה של פעילות חשודה (Tarpitting\Tarpits). ככלל, שימוש ב-IPS המובנה ב-FW הארגוני אינו מבטיח רמת עמידות הזהה לזו בעת שימוש ב-IPS ייעודי.
13.	מומלץ כי הארגון יוודא באופן עיתי כי חוקי הגישה ב-FW הארגוני (Ingress\Egress Filtering) עונים לעקרון מתן הרשאות גישה נמוכות (Least Privilege Access).
14.	מומלץ כי הארגון יוודא באופן עיתי כי מנגנון מניעת התחזות (Anti-Spoofing) מופעל ב-FW וה-IPS. בכלל זה, מומלץ לוודא כי לא ניתן ליצור קשר מהאינטרנט לנכסי הארגון באמצעות כתובות IP שמורות. להלן דוגמא לכתובות IPv4 שמורות: (0/8) loopback (127/8), private (RFC 1918 blocks 10/8, 172.16/12, and 192.168/16 ,(unassigned DHCP clients (169.254.0.0/16), multicast (224.0.0.0/4) and otherwise listed in RFC 5735 ו-כתובות IP v6 רלוונטיות: https://www.ripe.net/manage-ips-and-asns/ipv6/ipv6-address-types/ipv6addresstypes.pdf

מס'	ההמלצה
.15	מומלץ כי הארגון יוודא החלת הגבלת תעבורה (Rate Limit) כאמצעי הגנה על נכסי הסייבר השונים (לרבות נתבי התקשורת עצמם).
.16	מומלץ כי הארגון יעשה שימוש במערכת לתעדוף תעבורה נכנסת/יוצאת (QoS), וזאת בהתאם לצורכי הארגון.
.17	מומלץ כי הארגון יבצע הקשחה של נתבי תקשורת הנתונים, וזאת בהתאם להמלצות היצרן להתמודדות עם תקיפות מניעת שירות מבוזרות.
המלצות לאבטחת השכבה החיצונית (External Layer)	
.18	מומלץ כי הארגון יוודא כי ניתן לבצע הגדלה דינמית ומידית של רוחב הפס לאינטרנט. בכלל זה, יש לוודא כי נכסי הסייבר השונים תומכים ברוחב הפס הנדרש/החריג.
.19	מומלץ כי הארגון יעשה שימוש במספר ספקי שירותי אינטרנט שונים, אשר עושים שימוש בתשתית בלתי תלויה לשם גישה מחוץ לישראל.
.20	בעת עבודה עם שירותי ענן ציבוריים, מומלץ כי הארגון ינקוט בפעולות הבאות: א. קישור הארגון לספק הענן באמצעות שימוש בערוץ תקשורת שאינו נגיש ישירות לאינטרנט. דוגמא ליישום: שימוש ב-MPLS. ב. בחינת היצע שירותי ההגנה הזמינים בספק, תוך וידוא התאמתם לצורכי הארגון. ראוי לציין כי חבילות הבסיס מציעות בד"כ רמת הגנה נמוכה, אשר אינה כוללת מענה לתקיפת מניעת שירות מבוזרת המתמקדת ברמה האפליקטיבית.
.21	מומלץ כי הארגון יבקש מספק שירותי האינטרנט לבצע את הפעולות הבאות (Clean Pipe): א. מתן גישה בהתאם למודל "גישה מבוססת סיכון מסתגל". ראו לעיל.

מס'	ההמלצה
	ב. מתן גישה לפורטים/שירותים ספציפיים בלבד (Ingress\Egress Filtering). ג. תמיכה ביכולת העברת תעבורה חשודה/זדונית לבולען (Sinkhole) ול"חור שחור" (Blackholing). ד. מתן יכולת לארגון לבצע פעולות אִפְחוּת עצמאית, וזאת בהתאם לפרופיל האיומים הארגוני. ה. תמיכה באינטגרציה מול פתרון ניקוי בענן (Scrubbing[4]) של הספק ו/או גורם צד-שלישי.
22.	מומלץ כי הארגון יגן על תשתית ה-BGP. להרחבה ראו: מניעה והתמודדות כנגד חטיפת BGP - המלצות ליישום https://www.gov.il/he/departments/general/bgp
23.	מומלץ כי הארגון יעשה שימוש בפתרון ניקוי בענן (Scrubbing) כבקרה מפצה. ככלל, יש להעדיף להשתמש ב-BGP Redirect, ולא DNS Redirect, וזאת לאור העובדה כי האחרון משאיר את כתובת ה-IP הציבורית של הארגון חשופה לתקיפות. יש לבחון האם הצורך בפתרון הינו קבוע, או שניתן להפעילו רק במקרה של חשד/אירוע סייבר.
24.	מומלץ כי הארגון יוודא כי תשתית ה-DNS הציבורית של הארגון כוללת את היכולות הבאות: א. ביזור אופטימלי באתרים שונים ברחבי העולם. ב. תמיכה ב-GSLB\GeoDNS. ג. הגנה מובנית בפני תקיפות מניעת שירות מבוזרות.

[4] Cloud Scrubbing Center (CSC)

מס'	ההמלצה
	בקרה רצופה ומתמשכת (Continuous Monitoring)
.25	מומלץ כי הארגון יעשה שימוש במערכת לבחינת חווית לקוח (User Experience) בעת גישה מהאינטרנט, וזאת לשם גילוי וזיהוי סממנים העשויים להעיד על תקיפת מניעת שירות מבוזרת. דוגמא ליישום: שימוש במערכת APM (Application Performance Management).
.26	מומלץ כי הארגון יבצע ניטור רציף לטופולוגית ה-BGP המשפיעה על תשתית הארגון.
.27	מומלץ כי הארגון יאסוף וינתח את הארטיפקטים (Artifacts) משלוש השכבות: א. השכבה הפנימית ב. שכבת הקצה ג. השכבה החיצונית יוער כי לשם איסוף מידע מהשכבה החיצונית, הארגון עשוי להידרש לבצע פעולות איסוף באמצעות תשאול API's של הגורמים הרלוונטיים.
.28	מומלץ כי הארגון יינטר את האינדיקטורים ב**נספח א'**.
.29	מומלץ כי הארגון יאסוף טלמטריה (Telemetry) מנכסי הסייבר השונים, וזאת לשם גילוי וזיהוי מיטבי של ה-TTP's. יש לוודא כי הפתרון אשר נעשה בו שימוש בעל יכולת לייצר נראות (Visibility) מקצה לקצה, תוך מודעות למצב האפליקציה (Application State-Awareness).
.30	בעת עבודה עם ענן ציבורי, מומלץ כי הארגון יבצע איסוף נתונים אודות שינויים בזמן אמת של מרכז הרווח (Cost Center) באמצעות תשאול ה-API של הספק.
.31	מומלץ כי הארגון יבצע בחינה עיתית מהאינטרנט לגילוי וזיהוי IOE's אשר תוקף פוטנציאלי עשוי לנצלם לשם הגדלת אפקטיביות תקיפת

מס'	ההמלצה
	מניעת שירות, ובהתאם לנקוט בפעולות מתקנות. לשם גילוי וזיהוי IOE's ניתן לעשות שימוש בשירות SRS (Security Rating Services) או לעשות שימוש בפתרון אחר.
מוכנות לאירוע סייבר	
32.	מומלץ כי הארגון יעדכן את תוכנית ההמשכיות העסקית (BCP) בתרחישים רלוונטיים, ולוודא כי ברשות הארגון נוהל עבודה סדור של מקרים/תגובות.
33.	מומלץ כי הארגון יוודא כי ברשותו אמצעי מקובל להקלטת תעבורה (PCAP) המגיעה למבואות הארגון. דוגמא ליישום: שימוש ב-TAP או NPB.
34.	מומלץ כי הארגון יבצע תרגולות עיתיות לבחינת רמת הכשירות והמוכנות של הארגון, והגורמים המשיקים (דוגמת ספק האינטרנט). להלן דוגמא לתרחישים לבחינה: א. הגדלת רוחב הפס באופן מידי. ב. ביצוע בדיקת עומסים (Stress Test) וזאת לשם בחינת רמת העמידות של נכסי הסייבר. ג. ביצוע תרגיל שולחני (Tabletop Exercise) לתרגול יישום נוהל התגובה לאירועי תקיפת מניעת שירות מבוזרת ע"י הגורמים הרלוונטיים בארגון. ד. ביצוע חסימה יזומה של תוקף פוטנציאלי ברמת הארגון, ברמת ספק שירותי האינטרנט (לפי ACL), וברמת ספק פתרון הניקוי בענן (Scrubbing). ה. דילוג לעבודה לאתר חלופי (DR Site). ו. מעבר יזום לעבודה מול פתרון ניקוי בענן (Scrubbing), וחזרה.

מס'	ההמלצה
	נספח 2 מכיל דגשים לספר מרשם (Playbook) לתגובה בעת תקיפת מניעת שירות. להרחבה ראו: תרגול בסייבר - בנייה ועריכה של תרגילי סייבר לארגון https://www.gov.il/he/departments/general/cyberexercise
שרשרת האספקה	
35.	מומלץ כי הארגון יעגן משפטית את דרישות האבטחה לעיל מול ספקי השירות הרלוונטיים. יש לוודא החלת מדדים מקובלים בהסכם ההתקשרות, וזאת דוגמת: א. הזמן הנדרש לגילוי וזיהוי תקיפה (Time to Detect Attack). ב. הזמן האפקטיבי לביצוע אִפְחוּת (Time to Apply Effective Mitigation). ג. הזמן הנדרש לביצוע פעולות אִפְחוּת אפקטיביות (Time to Apply Effective Mitigation). ד. הזמן הנדרש לשליחת התרעה (Time to Alert) לגורמים הרלוונטיים. ה. הזמן הנדרש להסטת התעבורה לספק הניקיון (Time to Initiate Diversion). ו. היחס בין התעבורה הזדונית שעברה, לתעבורה הזדונית שנחסמה (Consistency of Mitigation). ז. זמינות שירותי ההגנה (Service Availability).
36.	מומלץ כי הארגון יעגן משפטית כי ספקי פתרונות ההגנה יחויבו להמציא לארגון חתימה לתקיפה חדשה בהתאם לסד זמנים הקבוע באמנת שירות (SLA). בכלל זה, יש לוודא כי ישנו תהליך מוסדר אשר במסגרתו הארגון ממציא לספק הפתרון הקלטה של התקיפה (PCAP), והספק מייצר חתימה בהתאם.

מס'	ההמלצה
37.	מומלץ כי הארגון יוודא כי ספקי השירות הרלוונטיים עומדים בדרישות מתודת שרשרת האספקה[5] של המערך.

טבלה 4: המלצות ליישום לשם היערכות כנגד תקיפות מניעת שירות מבוזרות (DDoS)

בעת עבודה עם אמצעי אבטחה צד-שלישי ניתן להגדיר כי פעולתם תהיה רציפה (Always-on) או שהם יכנסו לפעולה רק במקרה של חשד לקיום אירוע סייבר (On-Demand). על הארגון לגבש את אסטרטגיית היישום המתאימה לו, וזאת לאור ההשלכות הנגזרות.

[5] שאלון ספקים לחיזוק שרשרת האספקה
https://www.gov.il/he/departments/news/querysupply

7. נספחים (Appendixes)

פרק זה מכיל את רשימת הנספחים הנלווים למסמך זה.

נספח 1 - אינדיקטורים מומלצים לניטור

מטרת הנספח

להציג לקורא רשימת אינדיקטורים לדוגמא אשר מומלץ לנטר ב"זמן אמת" (Real Time):

מס'	האינדיקטור
	תקשורת נתונים
1.	עלייה חריגה בצריכת רוחב פס מ/אל האינטרנט (ברמת נכס סייבר ספציפי, צבר נכסי סייבר או כלל נכסי הסייבר).
2.	גישה חוזרת ונשנית באמצעות פורטי תקשורת חריגים (דוגמת ICMP).
3.	עלייה חריגה במספר הפעמים שבו תהליך ה-TCP Handshake אינו מושלם כיאות.
4.	עלייה חריגה במספר הניתוקים זמן קצר לאחר השלמת תהליך ה- TCP Handshake.
5.	עלייה חריגה במספר ה-Packet Loss.
6.	ייזום גישה עצמאית לאינטרנט ע"י נכסי הסייבר הממוקמים בשכבה הפנימית ו/או בשכבת הקצה.
7.	סריקת פורטים חוזרת ונשנית.
8.	אי תאימות בין מספר פורט התקשורת לסוג האפליקציה העושה בו שימוש (Mismatched Port-Application Traffic). דוגמא ליישום: גישה לאתר ה-Web באמצעות TCP 80, כאשר תוכן התעבורה הינו אפליקציית

	.FTP
.9	שימוש חוזר ונשנה עם HTTP Method שאינו מקובל באתר.
.10	אנומליה בתדירות שליחת פקטות מידע עם גודל חריג במסגרת חלון זמן מוגדר.
.11	אנומליה בגודל HTTP Query/Response במסגרת חלון זמן מוגדר.
.12	אנומליה בגודל DNS Query/Response במסגרת חלון זמן מוגדר.
.13	אנומליה במספר בקשות לקוח (DNS\HTTP etc.) במסגרת חלון זמן מוגדר.
.14	גישה מכתובות IP בעלות רמת אמון נמוכה (מוניטין נמוך) - דוגמת כתובת IP המשויכת לשרת פרוקסי אנונימי, שיוך לקמפיין תקיפה מוכר.
.15	שידור מחדש של מסר ישן (Replay-Attack).
.16	מספר חריג של קישורים מכתובת IP יחידה.
.17	מספר חריג של פקטות בעלות TTL=0.
נכסי סייבר - אפליקציה וניהול פעילות (Session)	
.18	עלייה חריגה בצריכת משאבים של נכס סייבר ספציפי, צבר נכסי סייבר או כלל נכסי הסייבר. דוגמא ליישום: א. עלייה חריגה במספר פעולות הקריאה/כתיבה לדיסק ו/או מסד נתונים. ב. עלייה חריגה במספר הפעמים בהם מתבצעת פעולת חזרה לאחור של לוגים (Log Rollbacks) בשרת מסד נתונים. ג. עלייה חריגה בצריכת שטח דיסק.

	ד. עלייה חריגה בצריכת ה-RAM. ה. עלייה חריגה במספר הקישורים. ו. עליה חריגה בזמן ה-TCP Connection. ז. עלייה חריגה במספר פקטות המידע. ח. עליה חריגה במספר בקשות HTTP\S או פרוטוקול רלוונטי אחר.
.19	עלייה חריגה במספר הפעולות של הוספה/הסרה של פריטים בעגלת הקניות של משתמשים באתר (Cart\Inventory Hoarding).
.20	עלייה חריגה במספר הטעויות בהקשת פרטים של כרטיסי מכירה (Gift Card Cracking).
.21	עלייה חריגה במספר הפעולות של הוספה/הסרה של פריטים בעגלת הקניות של משתמשים באתר (Cart).
.22	אנומליה במשך זמן הפעילות (Session) הממוצע של משתמשים.
.23	פניות חוזרות ונשנות של חשבון משתמש לגיטימי לנכסי הסייבר של הארגון ממקומות שונים גיאוגרפית בחלון זמן קצר (Geo-Velocity).
.24	גישה מנכס סייבר העושה שימוש בסוכן משתמש (User-Agent) שאינו מקובל.
.25	גישה מנכס סייבר העושה שימוש בסוכן משתמש (User-Agent) של מנוע חיפוש מקובל, אך כתובת ה-IP אינה משויכת בהתאם לפרסומי היצרן למנוע החיפוש. ניתן לבצע זאת ע"י Reverse Lookup או באמצעות דרך אחרת.
.26	גישה מנכס סייבר אשר הדפדפן שלו אינו מספק פונקציונליות הזהה לזו הקיימת בגרסה רשמית של היצרן. דוגמא ליישום: בחינת תקינות ה-DOM Tree בצד הדפדפן.
.27	עלייה חריגה במספר פעולות האימות המוצלחות / הלא מוצלחות ביחס

	לחלון זמן נתון.
.28	עלייה בשכיחות ב-Null Referrers בלוגים של שרת Web.
.29	עלייה בשכיחות שליחת HTTP status codes חריגים לבקשות משתמשים, בדגש על: Redirects (399-300) Client errors (499-400) Server errors (599-500)
.30	קריסה או אתחול לא מתוכנן של נכסי סייבר / שירותי מערכת.
.31	עלייה בזמן התגובה הממוצע לבקשת לקוחות חדשים/קיימים.
.32	הוצאות כספיות חריגות בגין שימוש בשירותי ענן ציבוריים.

טבלה 5: המלצות ליישום לשם היערכות כנגד תקיפות מניעת שירות מבוזרות (DDoS)

נספח 2 - דגשים לספר מרשם (Playbook) לתגובה בעת תקיפת מניעת שירות מבוזרת

מטרת הנספח

להציג לקורא דגשים לספר מרשם (Playbook) לתגובה בעת תקיפת מניעת שירות מבוזרת:

מס'	פעולה לביצוע
פעילות פנים ארגונית	
1.	מומלץ כי הארגון ישלח למקבלי ההחלטות (גורמים עסקיים, צוות ניהול משברים, דוברות וכד') התרעה אודות התקיפה, וזאת תוך התייחסות לנושאים מקובלים, דוגמת: א. נכסי הסייבר והתהליכים העסקיים המושפעים מהתקיפה ו/או העשויים להיות מושפעים ב. עצימות התקיפה וההשלכות העסקיות הנגזרות/בקרת נזקים ישירים ועקיפים (דוגמת נטישה של X לקוחות בדקה או הפסד כספי של Y שקלים). ג. הזמן בו צפוי כי התקיפה תשפיע על הארגון (ככל שניתן לחזות בהתאם לאירועים קודמים בעולם, לדוגמא) ד. קהל יעד מושפע (לקוחות פנימיים/חיצוניים, ספקים וכד') ה. הרף בו אמצעי האבטחה של הארגון לא יהיו אפקטיביים דיים, וזאת ביחס לנקודת זמן נתונה.
2.	מומלץ כי הארגון יגביר את רמת הכוננות של הגורמים הפנימיים, דוגמת ערוצי שירות חלופיים (דוגמת מוקד טלפוני אשר יתכן שיידרש להתמודד עם רף שיחות חריג הנובע מפניות לגיטימיות של לקוחות או פניות יזומות מצד תוקף אשר מטרתן לפגוע בזמינות ערוץ השירות הטלפוני במקביל לערוצי שירות מקוונים באינטרנט), מערכות המידע וצוות הגנת הסייבר (בדגש על צוות ניטור סייבר).

.3	מומלץ כי הארגון יבצע בדיקות לשם איתור שינויים לא רצוניים ואנומליה בנכסי הסייבר, אשר עשויים להצביע כי תקיפת מניעת השירות המבוזרת מהווה מסך עשן לתקיפה האמיתית.
.4	מומלץ כי הארגון יפרסם עדכון למשתמשים בארגון אודות התקיפה, והתנהלות מצופה מצדם.
.5	מומלץ כי הארגון יגדיל את קיבולת התשתיות הטכנולוגיות וזאת במטרה לפצות על הפגיעה ברמת השירות אשר התקיפה יוצרת. לדוגמא: א. הוספת שרתי Web נוספים. ב. הגדלת רוחב פס לאינטרנט. ג. מעבר לעבודה בענן ציבורי.
.6	מומלץ כי הארגון יוודא הפעלה של אמצעי האבטחה הקיימים ברשותו, לרבות מעבר יזום (בהתאם לצורך) לעבודה מול פתרון ניקוי בענן (Scrubbing). כמו כן, יש לבצע בקרה רציפה ומתמשכת רצופה של רמת האפקטיביות של אמצעי האבטחה.
.7	מומלץ כי הארגון יבצע הקלטה של התעבורה (PCAP), וזאת במטרה לאפשר יצירה חתימה ייעודית לתקיפה חדשה.
.8	מומלץ לבחון אפשרות לביצוע פעולות הכלה (Containment). להלן דוגמאות לפעולות הכלה שכיחות: א. דילוג לעבודה בענן ציבורי / אתר צל (Shadow Site). ב. ניתוק נכסי סייבר לא חיוניים מרשת האינטרנט. ג. עצירת תהליכי שדרוג מערכות ותשתיות.
פעילות מול גורמי-חוץ	
.9	מומלץ כי הארגון יבחן פרסום התרעה לקהלי יעד מושפעים. לדוגמא: א. פרסום התרעה באתר האינטרנט של הארגון אודות איטיות אפשרית

	בעת גישה לשירותים, והפנייתם לערוצי שירות חלופיים. ב. עדכון רגולטורים רלוונטיים. ג. עדכון גורמי תמיכה חיצוניים. ד. ספקים מהותיים בציר שרשרת האספקה.
.10	מומלץ כי הארגון יעדכן את ספק מודיעין איומים בסייבר אודות התקיפה.
.11	מומלץ כי הארגון יעדכן את מערך הסייבר הלאומי אודות התקיפה. מוקד טלפוני 119.
פעילות מול ספק שירותי האינטרנט	
.12	מומלץ כי הארגון יפנה לספק שירותי האינטרנט ויעדכן אותו אודות התקיפה, וזאת תוך מימוש משותף של בקרות הגנה מקובלות ברמת הספק. לדוגמא: חסימת טווח כתובות IP אשר התוקף עושה בו שימוש.
.13	מומלץ כי הארגון יבקש מספק שירותי האינטרנט כי יפנה לספקי המשנה שלו, וזאת במטרה לחסום את התקיפה ברמת ספק המקור, ונקיטה בפעולות להסרת אחיזת התוקף מהרשת.
פעילות בסוף אירוע	
.14	מומלץ כי הארגון יבצע תהליך בקרת נזקים ישירים ועקיפים (לרבות ביצוע פעולות התאוששות במקרה הצורך, ובחינת השפעה אפשרית על ערך המניות).
.15	מומלץ כי הארגון יבצע צייד איומים (Threat Hunting), וזאת במטרה לגלות ולזהות אחיזה אשר יתכן כי הושארה ע"י התוקף, אך מערכות האבטחה הקיימות אינן מסוגלות לגלות ולזהות את קיומה.
.16	מומלץ כי הארגון יעדכן את גורמי פנים/החוץ אודות סוף אירוע.

.17	מומלץ כי הארגון יבחן את רמת אפקטיביות מערך האבטחה (לרבות ספקי השירות הרלוונטיים), וזאת ביחס למדדים אשר אושרו במקור ע"י הנהלת הארגון. להלן דוגמא למדדים מקובלים: א. הזמן הנדרש לגילוי וזיהוי תקיפה (Time to Detect Attack). ב. הזמן האפקטיבי לביצוע אִפְחוּת (Time to Apply Effective Mitigation). ג. הזמן הנדרש לביצוע פעולות אִפְחוּת אפקטיביות (Time to Apply Effective Mitigation). ד. הזמן הנדרש לשליחת התרעה (Time to Alert) לגורמים הרלוונטיים. ה. הזמן הנדרש להסטת התעבורה לספק הניקיון (Time to Initiate Diversion). ו. היחס בין התעבורה הזדונית שעברה, לתעבורה הזדונית שנחסמה (Consistency of Mitigation). ז. זמינות שירותי ההגנה (Service Availability).
.18	מומלץ כי הארגון יבצע הפקת מסקנות ולקחים (Lesson Learned) וזאת לשם שיפור יכולת התגובה לאירועים עתידיים.

טבלה 6: ספר מרשם (Playbook) לתגובה בעת תקיפת מניעת שירות

נספח 3 - היערכות כנגד תקיפות מניעת שירות מבוזרות (DDoS)

מטרת הנספח

לשקף לקורא את אופן פיתוח המסמך, הגורמים המעורבים בתהליך כתיבתו ובהעברת משוב על התכנים לטובת מתן שקיפות וגילוי נאות לתהליך ולגורמים המעורבים על סוגיהם.

א. כיצד גובש המסמך - סקר שוק/סילבוס/השוואה בעולם

1) בחינה של תיעוד/תקינה מהעולם כגון NIST, ISO, ועוד (דוגמאות עיקריות מוצגות במסמך בפרק "מסמכים ישימים").
2) בחינה של פרסומים מקובלים בתחום (דוגמאות עיקריות מוצגות במסמך בפרק "מסמכים ישימים").
3) קבלת משוב מהציבור לטיוטות המסמך אשר פורסמו:

א. חברת Allot
ב. חברת F5 Network
ג. חברת Imperva
ד. חברת Radware
ה. מר דניאל ארנרייך - יועץ ומרצה בתחום הגנת מידע וסייבר

8. קיצורי שמות (Acronyms)

פרק מציג את קיצורי השמות בהם נעשה במסמך זה.

שם המונח	ביאור
דוא"ל	דואר אלקטרוני
ABAC	Attribute-Based Access Control
ACL	Access Control List
ADC	Application Delivery Controllers
API	Application Programming Interface
APM	Application Performance Management
ASN	Autonomous system Number
B2B	Business to Business
BCP	Business Continuity Planning
BGP	Border Gateway Protocol
bps	Bits Per Second
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CDN	Content Delivery Network
CSC	Cloud Scrubbing Center
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoH	DNS over HTTP
DoS	Denial of Service
DR	Disaster Recovery
EDoS	Economic Denial of Sustainability
FQDN	Fully Qualified Domain Name
GB/s	Gigabyte per Second
GSLB	Global Server Load Balancing
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilation, and Air Conditioning
ICAP	Internet Content Adaptation Protocol
IEEE	Institute of Electrical and Electronics Engineers
IOA	Indicator of Attack

שם המונח	ביאור
IOC	Indicator of Compromise
IOE	Indicator of Exposure
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
MiTM	Man-in-the-Middle Attack
MPLS	Multiprotocol Label Switching
MTBF	Mean Time Between Failures
MTU	Maximum Transmission Unit
NPB	Network Packet Broker
OSI	Open Systems Interconnection
PFC	Priority Flow Control
pps	Packets Per Second
QoS	Quality of Services
RAdAC	Risk Adaptive-Based Access Control
RAM	Random-Access Memory
RASP	Runtime Application Self-Protection
RPO	Recovery Point Objective
rps	Requests Per Second
RTO	Recovery Time Objective
RTT	Round-Trip Delay
SaaS	Software as a Service
SDK	Software Development Kit
SLA	Service Level Agreement
SRS	Security Rating Services
TBps	Terabytes per Second
TTL	Time to Live
TTM	Time to Mitigation
TTP	Tactics, Techniques and Procedures
URL	Uniform Resource Locator
VoIP	Voice Over IP

שם המונח	ביאור
VPN	Virtual Private Networking
WAF	Web Application Firewall

טבלה 7: קיצורי השמות בהם נעשה שימוש במסמך זה

9. מסמכים ישימים (Applicable Documents)

פרק זה מכיל את מקורות המידע עליהם הסתמכו הכותבים בעת כתיבת המסמך.

מקורות מידע בעברית:

מערך הסייבר הלאומי

מניעה והתמודדות כנגד חטיפת BGP - המלצות ליישום

- ✓ https://www.gov.il/he/departments/general/bgp

פיתוח מאובטח - עבודת מנהל הגנת סייבר CISO עם גופי הפיתוח בארגון

- ✓ https://www.gov.il/he/departments/general/securedevelopment

חיזוק זיהוי משתמשים במערכות ותשתיות של ארגונים ע"י שימוש באימות רב-גורמי (MFA)

- ✓ https://www.gov.il/he/departments/general/mfa

תרגול בסייבר - בנייה ועריכה של תרגילי סייבר לארגון

- ✓ https://www.gov.il/he/departments/general/cyberexercise

שימוש בשירותי ענן - הרחבה לתורת ההגנה בסייבר לארגון

- ✓ https://www.gov.il/he/departments/policies/cloud_services

תורת ההגנה בסייבר לארגון

- ✓ https://www.gov.il/he/departments/policies/cyber_security_methodology_for_organizations

תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר

- ✓ https://www.gov.il/he/Departments/news/cybercrisispreparedness

שאלון ספקים לחיזוק שרשרת האספקה

- ✓ https://www.gov.il/he/departments/news/querysupply

מתקפות מניעת שירות מבוזרות (DDoS) - פתרונות טכנולוגיים אפשריים

- ✓ https://www.gov.il/he/departments/publications/reports/ddos_solutions

כללי

התקפת מניעת-שירות, וכיצד האינטרנט בחוף המזרחי - הושבת?
http://www.softwarearchiblog.com/2016/10/ddos.html

Digital Whisper

מתקפות מניעת שירות מוגברות' רזיאל בקר ואיתי חורי, Digital Whisper, גליון 75, ספטמבר 2016

https://www.digitalwhisper.co.il/files/Zines/0x4B/DW75-4-AmplifiedDDoS.pdf

פוטנציאל מתקפות ה DDoS-במרחב האינטרנט הישראלי, יורי סלובודיאניוק , Digital Whisperגליון 54, אוקטובר 2014 ,

https://www.digitalwhisper.co.il/files/Zines/0x36/DW54-3-DDoS.pdf

מקורות מידע באנגלית:

General

Exponential growth in DDoS attack volumes

- ✓ https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks

Mitigating IoT-Based DDoS

- ✓ https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos

AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever

- ✓ https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

OWASP Automated Threat Handbook, v1.2, 2018

- ✓ https://github.com/OWASP/www-project-automated-threats-to-web-applications/tree/master/assets/files/EN

Worldwide DDoS Regulations

- ✓ https://government.cioreview.com/cxoinsight/worldwide-ddos-regulations-nid-146-cid-30.html

Re-Hash: The Largest DDoS Attacks in History

- ✓ https://www.thesslstore.com/blog/largest-ddos-attack-in-history/

The Top 10 DDoS Attack Trends

- ✓ https://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends_ebook.pdf

Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

- ✓ https://tools.ietf.org/html/bcp38

Top 15 Indicators Of Compromise

- ✓ https://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647

Understanding Denial-of-Service Attacks, Security Tip (ST04-015), CISA

- ✓ https://us-cert.cisa.gov/ncas/tips/ST04-015

HTTP response status codes

- ✓ https://developer.mozilla.org/en-US/docs/Web/HTTP/Status

Network Denial of Service, MITRE

- ✓ https://attack.mitre.org/techniques/T1498/

How to Fake Spoof your Location Google Chrome

- ✓ https://dowpie.com/fake-spoof-geo-location-google-chrome/

Guide to DDoS Attacks November, MS-ISAC 2017

- ✓ https://www.cisecurity.org/white-papers/technical-white-paper-guide-to-ddos-attacks/

IPv6 Address Types, RIPE
https://www.ripe.net/manage-ips-and-asns/ipv6/ipv6-address-

types/ipv6addresstypes.pdf

Allot

DDoS ATTACK HANDBOOK, Allot, 2018

- ✓ https://www.allot.com/docs/ddos-attack-handbook.pdf

Service Provider Requirements for DDoS Mitigation
Protecting and Optimizing Networks for Modern Threats
and Future Scale

- ✓ https://www.allot.com/resources/WP-Frost_Sullivan-DDoS-Mitigation-Requirements.pdf

Akamai

Making a DDoS Protection Plan 8 Best Practices

- ✓ https://www.akamai.com/uk/en/multimedia/documents/brochure/8-steps-to-a-ddos-mitigation-plan.pdf

Mitigating DDoS Attacks in Zero Seconds with Proactive Mitigation Controls

- ✓ https://www.akamai.com/uk/en/multimedia/documents/white-paper/proactive-ddos-mitigation-with-prolexic-mitigation-controls-whitepaper.pdf

F5

Mitigating Application DDoS Attacks

- ✓ https://www.brighttalk.com/webinar/mitigating-application-ddos-attacks/

Defeat BOT Attacks with NEW Silverline Shape Defense Managed Service

- ✓ https://www.f5.com/company/events/webinars/defeat-bot-attacks-with-new-silverline-shape-defense-managed-service

Blocking Bots: How Silverline Shape Defense Works

- ✓ https://devcentral.f5.com/s/articles/Blocking-Bots-How-Silverline-Shape-Defense-Works?srcHeader

Radware

A Snapshot of DDoS Regulations: 6 Protection Initiatives

- ✓ https://blog.radware.com/security/2014/05/snapshot-ddos-regulations/

DDoS Response Plan HOW TO PROTECT YOURSELF FROM DDOS ATTACKS BEFORE, DURING, AND AFTER AN ATTACK

DDoS Survival Handbook, Radware, 2013

- ✓ https://security.radware.com/uploadedFiles/Resources_and_Content/DDoS_Handbook/DDoS_Handbook.pdf

Gartner

DDoS: A Comparison of Defense Approaches, 24 April, 2020

- ✓ https://www.gartner.com/document/3907156

Solution Comparison for DDoS Cloud Scrubbing Centers, 16 April, 2020

- ✓ https://www.gartner.com/document/3983636

***** סוף מסמך *****