

הקדמה

מסמך זה מתבסס על "[תורת ההגנה בסייבר לארגון](#)" שפרסם מערך הסייבר הלאומי, ומפרט המלצות הגנה לעמדות הקצה.

המסמך מהווה המלצה לכלל הארגונים במשק הישראלי וניתן להשתמש בו לטובת העלאת החוסן בסייבר באופן חופשי.

המסמך מציג דרישות ההגנה בסיסיות הנדרשות בהתאם לפוטנציאל הנזק וארגונים נדרשים לבצע בנוסף באופן סדיר תהליך הערכת סיכונים ויישום של תוכנית הגנה מותאמת לארגונם.

המסמך פונה לכלל המשק ונכתב בלשון זכר מטעמי נוחות בלבד.

בשל אופיין הטכני של חלק מההמלצות נדרש לממשן על ידי אנשי מקצוע בעלי הכשרה וניסיון רלוונטיים.

מסמך זה נכתב ע"י מנהל אבטחת מידע בחשבשבת לטובת חיזוק אבטחת הסייבר במחשבי לקוחות החברה.

מטרת המסמך

מטרת המסמך היא להמליץ על אמצעים המאפשרים להגן על תחנות הקצה, על ידי יצירת מעגלי האבטחה הבאים: אבטחה פיזית ומניעת גישה, הרשאות, הגנת המידע ותוכנות אבטחה.

ניתן ליישם את המלצות המסמך בתחנות קבועות בארגון, בתחנות ניידות וכן בעת חיבור תחנות קצה, אשר אינן רכוש הארגון, לרשת הארגונית (כדוגמת BYOD).

המסמך מתייחס באופן כללי לתחנת קצה באשר היא, ללא תלות במערכת ההפעלה. עם זאת, מרבית הדוגמאות וצילומי המסך הובאו ממערכת "חלונות" שהיא מערכת ההפעלה הנפוצה ביותר עבור תחנות קצה.

לכללי הקשחת מערכת Windows ניתן לגשת לאתר - <https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines>

לכללי הקשחת תחנת לינוקס ניתן לגשת לאתר - <https://www.computerworld.com/article/3144985/linux/linux-hardening-a-15-step-checklist-for-a-secure-linux-server.html>

מיפוי גישה והזדמנויות תקיפה

תחנת הקצה היא אמצעי המחשוב עימה עובד המשתמש בארגון המהווה מטרה אטרקטיבית לתוקפים ויכולה לשמש כראש גשר לתקיפת הארגון.

במסמך זה נתייחס למחשבים אישיים כאל תחנת הקצה של העובד בארגון אותם ניתן לתקוף במגוון דרכים (ווקטורי תקיפה) ולטובת מספר מטרות:

- דרך החדרת אמצעי זיכרון פיזי - כדוגמת כונן נייד המכיל פוגען
- באמצעות קישור העמדה לרשת חיצונית (דוגמת האינטרנט)
- דרך גניבת עמדת הקצה (בעיקר אם היא ניידת)
- גישה לא מורשית לעמדה או פריצה פיזית או שילוב חומרה או תוכנה. לדוגמה - החדרת Keylogger ציטות או החדרת סוסט"ר לעמדה לצורך גניבת המידע שעל העמדה או לצורך דילוג למחשבים נוספים בארגון וכד'.

המלצות הגנה

1. **אבטחה פיזית ומניעת גישה תורת הגנה בסייבר לארגון > הגנה פיזית וסביבתית > 18.1**
עקרון ההקשחה - מניעת גישה מגורמים לא מורשים ואבטחה פיזית הינן אמצעי אבטחה בסיסיים שיש ליישם לצורך אבטחת תחנת הקצה. מטרתה למנוע אבדן או גניבה של חומרה, שיכול לגרום נזק עצום לארגון. לכן יש ליישם מנגנוני אבטחה פיזית לתחנות הקצה.

- תהליך ההקשחה - אבטחת פיזית של תחנת הקצה תבצע בכמה שכבות:**
- א. ברמת המתחם – יש לוודא שמתחם העבודה מוגן וכי הגישה אליו היא למורשים בלבד, לדוגמה: יישום מערכת בקרת כניסה מבוססת תגי קרבה.
 - ב. ברמת תחנת הקצה -
 1. שימוש בכלוב נעילה או שימוש בכבל נעילה כאמצעי מאסיבי וקבוע בתחנת העבודה. הדבר מונע אפשרות של ניתוק וגניבת העמדה ממקומה.
 2. שימוש במדיניות סיסמאות ונעילת תחנות הקצה עם סיסמה.
 3. יישום מנגנון הצפנה לדיסק הקשיח במחשבים ניידים.
 4. יישום מנגנון אוטומטי לנעילת תחנת הקצה לאחר פרק זמן מוגדר של אי שימוש.
- יש להקפיד על החתמת העובדים על מסמך נהלים להגנה ושמירה על עמדות העבודה.

2. גישה והרשאות תורת הגנה בסייבר > בקרת גישה > 4.9 , 4.10

2.1 עקרון ההקשחה- הפחתת הרשאות, השימוש בחשבונות בעלי הרשאות רחבות (חשבון מנהל) מהווים אחת מהמטרות המרכזיות של תוקפים בסייבר, מאחר שהם מאפשרים למי שמשיג גישה אליהם, השתלטות על תחנת הקצה וממנה השתלטות על כלל הרשת. אחד האמצעים הראשונים לצמצום משטח התקיפה הוא יצירת חשבון משתמש רגיל, עם הרשאות מצומצמות. שימוש במשתמש בעל הרשאות מוגבלות מקשה על הגורם התוקף להשיג הרשאות מנהל לביצוע שינויים רחבים במערכת ולהתבסס בתחנת הקצה.

תהליך ההקשחה:

- א. יש להפחית את כמות חשבונות המנהל בחשבשבת ובתחנת הקצה למינימום האפשרי.
- ב. הגדרת כניסה לתוכנה ע"י שימוש במשתמשי מערכת ההפעלה.
- ג. מומלץ לנטר ולהתריע על כל שינוי או הוספה של חשבונות פריוויליגיים.
- ד. שימוש במנגנון זיהוי רב שלבי (MFA) ככל שאפשר.

כללים לניהול סיסמא ניתן למצוא באתר- [HTTPS://WWW.NIST.GOV/BLOGS/TAKING-MEASURE/EASY-WAYS-BUILD-BETTER-P5WORD](https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5word)

3. הגנה על המידע תורת הגנה בסייבר > המשכיות עסקית

3.1 גיבוי מידע, עקרון ההקשחה - גיבוי המידע, תחנות הקצה בארגונים עלולות להכיל מידע רגיש רב, ולכן יכולות להיפגע מטעויות אנוש כמו מחיקה בשוגג של מידע או נזק בשל תקיפת סייבר. לדוגמה, כופרות ופוגענים אשר משביתים את המידע הקיים על תחנת הקצה באמצעות הצפנתו, ולעתים קרובות גם לאחר התשלום לא מתאפשרת גישה למידע, והמידע אובד. נוסף על השימוש באנטי-וירוס, הדרך היעילה ביותר להתמודדות עם תקיפה מסוג זה היא לבצע גיבוי למידע. כלל המידע החיוני לארגון חייב להיות מגובה באמצעים, אשר מאפשרים שחזור במקרה של פגיעה בתחנת הקצה.

תהליך ההקשחה - דרך ההתמודדות עם מתקפות מסוג כופרה היא גיבוי המידע באמצעי חיצוני - על גבי כונן רשת, כונן חיצוני או גיבוי בענן. חיבור אמצעי לתחנת הקצה ייעשה בזמן הגיבוי

בלבד, ובשאר הזמן על אמצעי זה להיות מנותק באופן קבע מתחנת הקצה, כדי שלא ייפגע במקרה של חדירת פוגען.

המלצות לניהול מדיניות גיבויים ניתן למצוא באתר-

[HTTPS://WWW.CISEcurity.ORG/CONTROLS/DATA-RECOVERY-CAPABILITY](https://www.cisecurity.org/controls/data-recovery-capability)

3.2 מניעת דלף מידע (DLP), עקרון ההקשחה - עובדים בארגון יכולים להוציא מידע רגיש אל מחוץ לארגון באמצעים שונים, כדוגמת: שליחה אמצעות מייל, העתקה להתקן USB ועוד. הוצאת מידע רגיש יכולה להתרחש בכוונת זדון או כתוצאה מטעות אנוש, לכן שכבת אבטחה מפני זליגת מידע מהארגון היא בעלת חשיבות רבה. פתרונות מסוג DLP מסייעים לארגון לבצע ניטור ולחסום העברת מידע אל גורמים בלתי מורשים, ובכך למזער תקריות של אובדן מידע רגיש ודליפתו. מערכת DLP יכולה לתעד את פעולות משתמש על תחנת הקצה ולבחון פעילות חשודה שיכולה להזיק לארגון, כגון מכירת ידע, ביצוע הונאות ופעולות זדוניות נוספות.

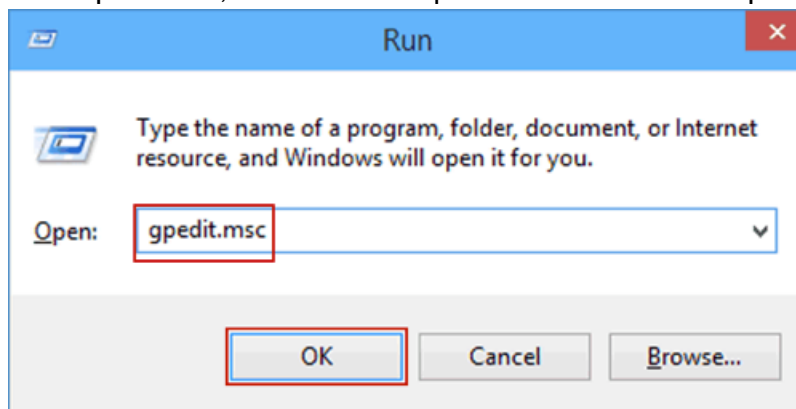
תהליך ההקשחה - והפעולות העיקריות שיש לבחון:

- מידור וביטול הרשאות גישה למידע לא נחוץ בהגדרות תוכנות עליהם עובדים.
 - קביעת מדיניות ניטור וחוקים רלוונטיים.
 - מעקב אחר גישה למידע רגיש וחסוי של הארגון.
 - ניטור העברה של מידע מתחנת הקצה להתקן חיצוני או למייל חיצוני.
 - התקנת מערכות DLP.
- המלצות להגנה מפני דלף מידע ניתן למצוא באתר-

[HTTPS://WWW.CISEcurity.ORG/CONTROLS/DATA-PROTECTION](https://www.cisecurity.org/controls/data-protection)

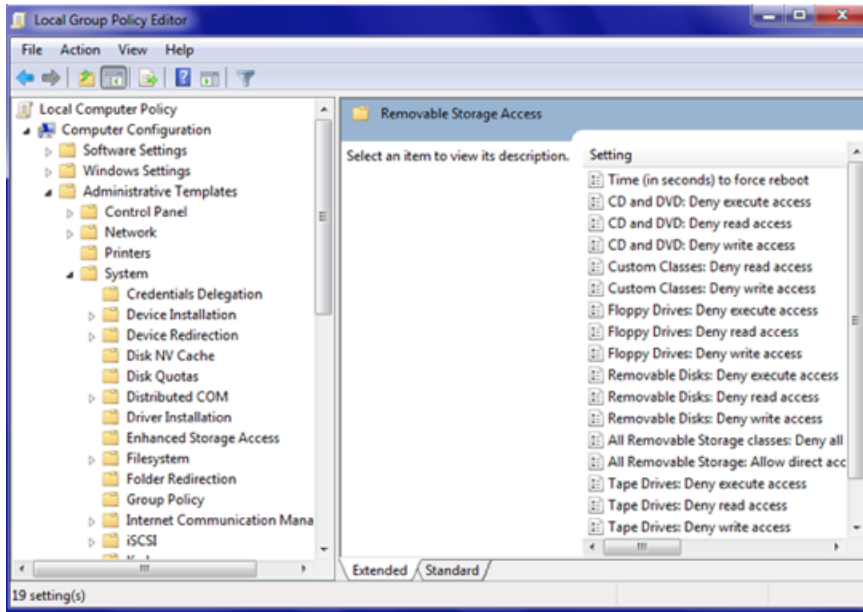
3.3 חסימת התקנים, עקרון ההקשחה - השימוש בהתקני זיכרון מבוססי USB נפוץ כיום. התקנים אלו מאפשרים העתקת מידע מהיר מהמחשב האישי אל כוננים חיצוניים, וכן שימוש בהתקנים נשלפים אחרים. באמצעות התקנים אלו ניתן להחדיר וירוס/ נזקה לכל מחשב המאפשר חיבור USB. כדי להגן על המידע הרגיש של הארגון יש להגביל את הגישה לחיבור התקנים מסוג זה בנקודת הקצה. קיימות שתי נקודות תורפה בהן רצוי להגן על תחנת הקצה: הגנה על המחשב והגנה על ההתקנים הניידים שאנו משתמשים בהם. תהליך ההקשחה- ביטול האפשרות לחיבור USB (ברשתות מבוססות דומיין MICROSOFT ניתן להגדיר חסימה ב-GPO):

- ראשית יש ללחוץ על מקש "התחל" ולאחר מכן, בשורת החיפוש, יש להקליד RUN:
- בחלון שייפתח יש לרשום את הפקודה: GPEDIT.MSC, ולאחר מכן OK.



- בחלון שייפתח יש לנווט אל תצורת מחשב > ADMINISTRATIVE TEMPLATES.
- המערכת תציג כמה אפשרויות – תחילה יש לבחור באפשרות SYSTEM

• לאחר מכן יש לבחור באפשרות STORAGE ACCESS.REMOVABLE



- כעת יופיעו 3 אפשרויות. יש לבחור בכל פעם באחת מהן על ידי לחיצה כפולה, ולסמן את האפשרויות הבאות:
 - REMOVABLE DISKS : DENY EXECUTE ACCESS
 - REMOVABLE DISKS : DENY WRITE ACCESS
 - REMOVABLE DISKS : DENY READ ACCESS

4. מניעת קוד זדוני תורת הגנה בסייבר לארגון > מניעת קוד > 7.8

4.1 אנטי-וירוס עקרון ההקשחה - שימוש בתוכנת אנטי-וירוס במטרה לאתר מתקפות מסוג וירוסים ופוגענים אחרים על תחנת הקצה, ולהגן מפעילותם. במצב אופטימלי, התוכנה תצליח לאתר ניסיון תקיפה על תחנת הקצה לפני שהגורם הזדוני יצליח לבצע התקנה על המחשב. במקרה שבו התחנה כבר "מזוהמת" בקובץ זדוני, האנטי-וירוס יכול לזהות את הקובץ הקיים בזמן פעולתו על המחשב בעזרת חתימות שונות ובחלק מהמקרים גם להסירו ולכן חשוב מאוד לעדכן באופן שוטף את תוכנת האנטי-וירוס.

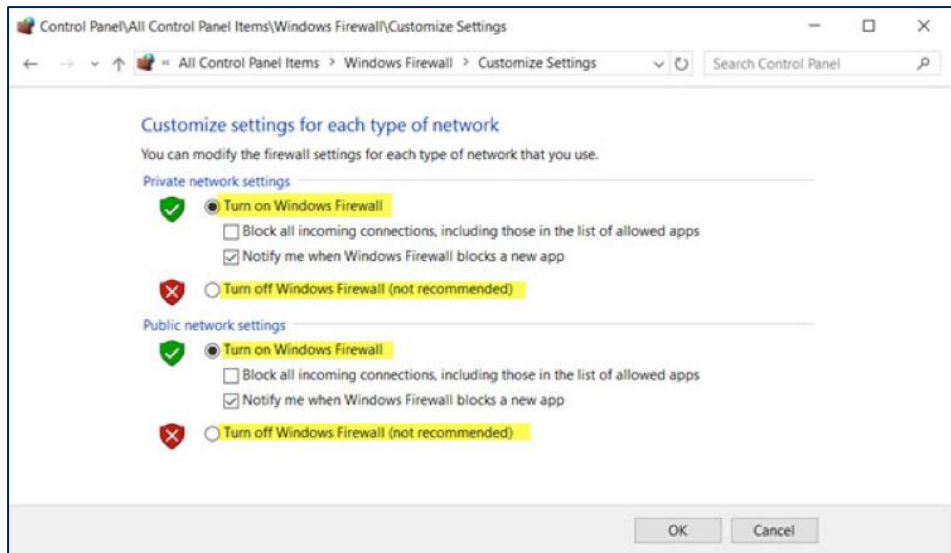
תהליך ההקשחה שיטות יישום באנטי וירוס

- א. יש להתקין תוכנת אנטי-וירוס של ספק מהימן בעמדת קצה.
- ב. יש לוודא עדכניות של תוכנת האנטי-וירוס באופן אוטומטי או יזום לפחות אחת ליום.

5. תורת הגנה בסייבר לארגון > הגנת תחנות עבודה ושרתים > 6.1

חומת אש עקרון ההקשחה- יישום ושימוש בחומת אש חיצונית ושל מערכות הפעלה בתחנות הקצה מאפשרת לחסום תעבורה לא חוקית אל תחנת הקצה וממנה חומת-האש נועדה להגן על הרשת באמצעות זיהוי תעבורה שאינה מאושרת וחסומתה, ועזרת לחסום תוכנות זדוניות, כגון וירוסים ופוגענים.

- תהליך ההקשחה- על מנת לוודא שחומת-האש אכן רצה ברקע, יש לפעול על פי סדר הפעולות הבא:
- יש ללחוץ על "התחל" ולאחר מכן לבחור באפשרות של לוח בקרה.
 - לאחר מכן יש לבחור באפשרות WINDOWS FIREWALL.
 - לוודא שהאפשרות שנבחרה היא: WINDOWS FIREWALL ON TURN מצד שמאל של המסך.
 - יש לוודא ששתי האפשרויות מסומנות כמו בתצלום הבא:



ל WINDOWS FW -יש שלושה פרופילים לסביבות שונות: PUBLIC ,PRIVATE ו- DOMAIN .
 מידע בנושא באתר [HTTPS://LEARN.MICROSOFT.COM/EN-US/PREVIOUS-VERSIONS/WINDOWS/DESKTOP/ICS/WINDOWS-FIREWALL-PROFILES](https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ics/windows-firewall-profiles)

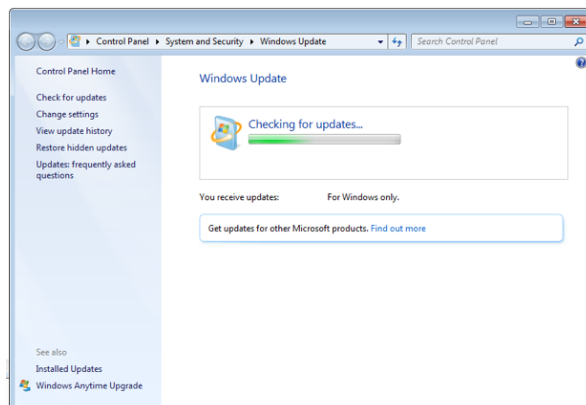
6. עדכוני אבטחה תורת הגנה בסייבר לארגון > מניעת קוד זדוני > 7.9

6.1 עדכוני אבטחה עקרון ההקשחה - בכל תוכנה מתגלים לעתים כשלים, שהתוקפים עלולים לנצלם לתקיפת תחנת עדכוני אבטחה למוצריהם. על מנת לסייע ללקוחותיהם לשמור על תחנות הקצה מוגנות, בפרט יצרני מערכות הפעלה, שהן רכיב התוכנה המרכזי בכל תחנת קצה, מספקים עדכוני אבטחה על בסיס קבוע ולעתים מפיצים עדכונים קריטיים בתדירות גבוהה אף יותר. ביצוע עדכונים באופן שוטף ממזער את האפשרות שתוקף ינצל חולשות אלו.

תהליך ההקשחה - יש לשאוף שעדכונים יותקנו באופן אוטומטי ללא התערבות המשתמש. עם זאת, במהלך כזה קיים סיכון, שעדכון ישבית את תחנת הקצה מסיבות שונות. בארגונים שבהם החומרה של התממשות סיכון זה היא קריטית, יש לבצע עדכונים באופן ידני ורק לאחר שנבדק כי אינם משביתים את תחנות הקצה. יש לבצע באופן שוטף עדכונים לתחנות הקצה על מנת למנוע מהתוקפים לנצל פרצות אלו.

כדי להפעיל את העדכון יש לבצע את הפעולות הבאות:

- יש ללחוץ על "התחל" > בלוח הבקרה
- בשורת החיפוש להקליד WINDOWS UPDATES
- יש לבחור באפשרות CHECK FOR UPDATES



טבלת עזר לביצוע הקשחות

מ.ס.	נושא	בוצע	חלקי	לא בוצע
.1	אבטחה פיזית של תחנות קצה			
.2	הקשחת BIOS			
.3	הצפנת דיסק קשיח			
.4	הפחתת חשבונות ADMIN			
.5	מדיניות סיסמאות			
.6	LOCAL ADMIN ביטול			
.7	התקנת "מלכודות דבש"			
.8	גיבוי מידע			
.9	מניעת דלף מידע			
.10	חסימת התקנים			
.11	התקנת אנטי-וירוס			
.12	התקנת מערכת EDR			
.13	הפעלת חומת-אש מקומית			
.14	הפעלת עדכוני אבטחה			