סייבר ישראל
משרד ראש הממשלה
מערך הסייבר הלאומי

המלצות הגנה

לצמצום סיכוני סייבר בתחנות הקצה בארגון

יוני 2018

סייבר ישראל
משרד ראש הממשלה
מערך הסייבר הלאומי

המלצות הגנה

לצמצום סיכוני סייבר בתחנות הקצה בארגון

יוני 2018

מסמך זה נכתב ע"י מערך הסייבר הלאומי לטובת הציבור. המסמך מהווה המלצה לכלל הארגונים במשק הישראלי. ניתן להשתמש בו לטובת העלאת החוסן בסייבר במשק באופן חופשי. מסמך זה נכתב עבור הנהלות של חברות, מנהלי הגנה בסייבר ומיישמים ואנשי IT. המסמך מציג את דרישות ההגנה המינימאליות הנדרשות בהתאם לפוטנציאל הנזק. ארגונים נדרשים לבצע תהליך הערכת הסיכונים ויכולים לבנות תוכנית הגנה מחמירה מדרישות מסמך זה. 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. התייחסויות למסמך ניתן להעביר במייל ל-tora@cyber.gov.il

כל הזכויות שמורות
למערך הסייבר הלאומי

תוכן העניינים

הקדמה 4
מטרת המסמך 5
קהל יעד 5
האיום 6
המלצות הגנה 7
1 אבטחה פיזית ומניעת גישה 7
2 גישה והרשאות 8
2.1 Secure Boot 8
2.2 הצפנת דיסק קשיח 8
2.3 הפחתת הרשאות 8
2.4 מדיניות סיסמאות 9
2.5 ביטול Local Administrator בתחנות הקצה 10
2.6 "משתמש דבש" (Honey Pot) 11
3 הגנה על המידע 12
3.1 גיבוי המידע 12
3.2 מניעת דלף מידע (DLP) 12
3.3 חסימת התקנים 13
4 תוכנות אבטחה 15
4.1 אנטי-וירוס (Anti-Virus) 15
4.2 מערכת EDR 16
5 Local Firewall 16
6 עדכוני אבטחה 17
נספח א' רשימת תיוג 19

הקדמה

תחנת הקצה היא אמצעי המחשוב עימה עובד המשתמש בארגון. באמצעותה העובד ניגש לתוכנות, לאפליקציות, למשאבי מידע ארגוניים ולצורך ביצוע תהליכים. ככזו תחנת קצה חשופה למגוון איומי סייבר הקשורים לשימוש העובד בעמדה, להגדרותיה ולקישורה לרשת הארגונית. מסמך זה מתבסס על "תורת ההגנה בסייבר לארגון"[1] שפרסם מערך הסייבר הלאומי, ומפרט המלצות הגנה לעמדות הקצה.

[1] https://www.gov.il/he/Departments/Guides/cyber_security_methodology_for_organizations_test

מטרת המסמך

מטרת המסמך היא להמליץ על אמצעים המאפשרים להגן על תחנות הקצה, על ידי יצירת מעגלי אבטחה 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.[2]

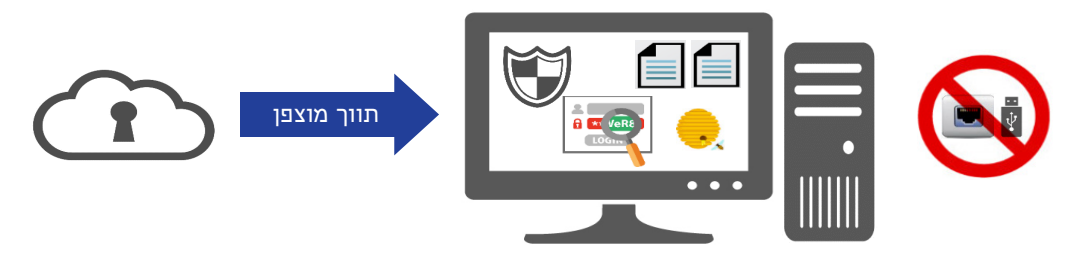
קהל יעד

מסמך זה מיועד למנהלי חברות, למנהלי IT ולמנהלי אבטחת מידע, המעוניינים לשפר את רמת אבטחת המידע בארגונם באמצעות שיפור רמת האבטחה בתחנות הקצה.
בשל אופיין הטכני של חלק מההמלצות נדרש לממשן על ידי אנשי מקצוע בעלי הכשרה וניסיון רלוונטיים.

[2] לכללי הקשחת מערכת Windows ניתן לגשת ל-
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines
לכללי הקשחת תחנת לינוקס ניתן לגשת ל-
https://www.computerworld.com/article/3144985/linux/linux-hardening-a-15-step-checklist-for-a-secure-linux-server.html

האיום

מיפוי גישה והזדמנויות תקיפה



תחנת הקצה מהווה מטרה אטרקטיבית לתוקפים ויכולה לשמש כראש גשר לתקיפת הארגון. במסמך זה נתייחס למחשבים אישיים כאל תחנת הקצה של העובד בארגון.

ניתן לתקוף עמדות קצה של הארגון 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 ציתות או החדרת סוסט"ר לעמדה לצורך גניבת המידע שעל העמדה או לצורך דילוג למחשבים נוספים בארגון וכד'.

המלצות הגנה

1 אבטחה פיזית ומניעת גישה

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 תתבצע בכמה שכבות:

א. ברמת המתחם - יש לוודא שמתחם העבודה מוגן וכי הגישה אליו היא למורשים בלבד, לדוגמה: יישום מערכת בקרת כניסה מבוססת תגי קרבה.

מערכת בקרת כניסה מבוססת תגי קרבה

ב. ברמת תחנת הקצה - שימוש בכלוב נעילה או שימוש בכבל נעילה כאמצעי מאסיבי וקבוע בתחנת העבודה. הדבר מונע אפשרות של ניתוק וגניבת העמדה ממקומה.

כבל נעילה לעמדת קצה

ג. יישום מנגנון אוטומטי לנעילת תחנת הקצה לאחר פרק זמן מוגדר של אי שימוש.

ד. יש להקפיד על החתמת העובדים על נהלים מתאימים להגנה ושמירה על העמדה (כדוגמת נעילה העמדה בסיסמה, מניעת גישה למתחם העבודה וכד').

שים לב! יש לוודא שקיימת מדיניות לשמירת אבטחה פיזית בארגון.

תורת הגנה בסייבר לארגון > משפחה: הגנה פיזית וסביבתית > 18.1

2 גישה והרשאות

2.1 Secure Boot

עקרון ההקשחה

Secure Boot הינה תכונה המיושמת במחשבי PC מתקדמים והמאפשרת לוודא, כי הרכיב הטוען את מערכת ההפעלה חתום ומאושר. כך נמנע מתוכנות זדוניות מסוג Rootkit לפעול ולשלוט בתחנת הקצה. יש להקפיד, כי בארגון תופעלנה אך ורק מערכות הפעלה אשר תומכות ב-Secure Bot.

תהליך ההקשחה

לרוב, כאשר מתקינים מערכות ההפעלה, תכונת Secure Boot מופעלת כברירת מחדל. כדי לא לאפשר לתוכנות זדוניות מסוג Rootkit לבסס אחיזה בתחנת הקצה, אנו ממליצים שלא לשנות הגדרה זו.[3]

שים לב! מומלץ לא לבטל את הגדרות ברירת המחדל של מערכת ההפעלה בהיבטי הגנה. לביטול זה ישנן השלכות על רמת האבטחה של תחנות הקצה.

2.2 הצפנת דיסק קשיח

עקרון ההקשחה

תחנות קצה בכלל, ומחשבים ניידים בפרט, נמצאים בסיכון לגניבה, לאובדן או לשכחה - דבר העלול לאפשר גישה למידע השמור בהם לגורם לא מורשה. הצפנת הדיסק הופכת את המידע בו ללא קריא למי שאינו מחזיק במפתח ההצפנה, ומפחיתה משמעותית את הסיכון של דלף מידע.

תהליך ההקשחה

לבעלי תחנות קצה המריצות את מערכת ההפעלה "חלונות" של Microsoft - היצרנית מספקת תוכנה להצפנת דיסק בשם BitLocker. בנוסף, קיימים פתרונות של יצרנים אחרים.

לבעלי תחנות קצה המריצות Linux - קיימים כלי Open Source להצפנת הדיסק.
חברת Apple מספקת פתרון בשם FileVault להצפנת הדיסק במחשבים מבוססי מערכת ההפעלה שלה.

שים לב! יש לוודא, כי הפתרון מצפין את כל הדיסק על מנת לוודא ששום מידע לא ידלוף במקרה של גניבה או אובדן של תחנת הקצה.

תורת הגנה בסייבר לארגון > משפחה: הצפנה > 8.7

2.3 הפחתת הרשאות

עקרון ההקשחה

חשבונות בעלי הרשאות רחבות (חשבונות פריווילגיים/Admin) 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, אשר ישמש לעבודה היומיומית.[4]
חשבון בעל הרשאות Admin ישמש רק בעת הצורך, לדוגמה - בעת התקנת תוכנות. הסיבה לכך היא, שאם תוכנה זדונית או תוקף יפגעו בתחנה, 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 בתחנת הקצה למינימום האפשרי (ראה סעיף 2.5 כיצד להגדיר חשבון מנהל).

[3] https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/disabling-secure-boot
[4] CIS Control 4 https://www.cisecurity.org/controls/controlled-use-of-administrative-privileges

ב. אין להגדיר את בעל העמדה כמנהל מקומי, אלא כמשתמש "רגיל".

ג. כל פעולה בתחנת הקצה יש לבצע באמצעות משתמש בעל ההרשאות הנמוכות ביותר, המאפשרות לבצע פעולה זו. במקרה של פעולות שמחייבות שימוש במשתמש פריווילגי, תבוצע הפעולה הספציפית בלבד. ניתן להשתמש במערכות להעלאת הרשאות על פי דרישה.

ד. מומלץ לנטר ולהתריע על כל שינוי או הוספה של חשבונות פריוליגיים.

שים לב! יש להתאים את ההרשאות בארגון לפי הצורך לתפקידים השונים (ולתת מינימום הרשאות לכל תפקיד).

תורת הגנה בסייבר לארגון > משפחה: בקרת גישה > 4.9, 4.10

2.4 מדיניות סיסמאות

עקרון ההקשחה

אחד מניסיונות הפריצה הראשונים והנפוצים מצד גורם זדוני לארגון הוא ניסיון תקיפה ופריצה של מנגנון הסיסמאות של הרשת הארגונית.

עקיפת מנגנון הסיסמאות תצמצם את הצורך בהשקעת משאבים וזמן לפריצת מנגנונים אחרים, כגון: הרשאות, מערכות, הצפנה. מטרתנו תהיה, לפיכך, להקשות על ניסיונות התוקף לעקוף את מנגנון הסיסמאות.

סיסמה קשה לפיצוח תקשה על התוקף לנחש אותה בזמן סביר. בחירת סיסמה טובה לא תשאיר בפני הפורץ ברירה, אלא לנסות את כל הסיסמאות האפשריות בעזרת Brute-force search (ובכך נגדיל את הזמן הנדרש להרצתו או נכשילו לחלוטין).

הידעת?

המושג **Brute-force** מתייחס לתהליך או לאלגוריתם, הפועל באופן של ניסוי וטעייה של כלל האפשרויות לפתרון בעיה נתונה עד למציאת הפתרון הנכון.

התקפת מילון (Dictionary attack) - שימוש בתוכנות לניחוש סיסמת משתמש נקרא גם "התקפת מילון". מדובר בניסיון ניחוש של סיסמת המשתמש על ידי Brute-force, קרי ניסוי ובדיקה של כל הסיסמאות האפשרויות, הסיסמאות הסבירות או הנפוצות ביותר, לרוב תוך שימוש בקבצים המכילים רשימות ארוכות של סיסמאות מסוגים אלו. תוקף יכול למצוא רשימות מסוג זה גם באינטרנט.

תהליך ההקשחה

א. להלן כללים בסיסיים לבחירת סיסמה:

- **ככלל, אין להתבסס רק על הסיסמה.** רצוי לשלב מנגנון אימות נוסף - כדוגמת אימות דו שלבי. [5]
- אין להשתמש בפרטי המשתמש בתוך הסיסמה, כגון: שם פרטי, שם משפחה, תאריך לידה, תעודת זהות, מספר טלפון וכדומה.
- הסיסמה תהיה מורכבת מ-8 תווים לפחות.
- יש להגדיר סיסמה שמכילה אותיות, תווים מיוחדים ומספרים.
- יש להימנע ממילים סטנדרטיות.
- יש להגדיר בנוהלי הארגון, כי סיסמה היא אישית ואין לשתף או להעבירה לשום גורם בארגון ומחוצה לו.

הערה: קיימות גישות והמלצות שונות כדוגמת המלצת ה- NIST ל-Passphrase. [6]

ב. מדיניות שיש לאכוף על החלפת סיסמה:

- יש להחליף סיסמה כל 90 יום.

[5] https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd

[6] https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd

- אין לחזור על סיסמאות שנעשה בהן שימוש בעבר.
- הגדרת נעילת משתמש לאחר 5 כישלונות. חשוב לוודא, שמנהל הרשת מחיל ברמת הרשת (Domain) ובעזרת GPO את מדיניות הסיסמאות שהארגון קבע, זאת על מנת לאכוף אותה בכל הרשת הארגונית.

ג. בדיקות רבעוניות, שיכולות להתבצע ע"י מנהל אבטחת המידע או צוות ה- Help Desk למדיניות ה-AD, במטרה לוודא שהמשתמש אכן עומד במדיניות:

- שדה Password Required: לוודא שכל המשתמשים מחויבים בהזדהות עם סיסמה.
- שדה Password Last Changed: לבדוק שלא קיימות שורות שהתאריך בהן הוא יותר מ-90 יום.
- שדה Password Expires: לאתר משתמשים בעלי הגדרה שאינה מחייבת החלפת סיסמה.

שים לב! חשוב לוודא, שתהליך ניהול הסיסמאות בארגון תואם למדיניות הסיסמאות שנקבעה על מנת להקשות על פריצה לארגון ולמנוע שימוש בנתונים אלו לרעה.

תורת הגנה בסייבר לארגון > משפחה: בקרת גישה > 4.35

2.5 ביטול Local Administrator בתחנות הקצה

עקרון ההקשחה

הרשאות מסוג Admin מקומי בתחנות הקצה מאפשרות שליטה כמעט מלאה על תחנות אלו, דבר שחושף את הרשת הארגונית לסיכון גבוה יותר.

Admin מקומי מקבל גישה לכל קובץ ויישום ברשת. כאשר הוא נתקל בבעיית הרשאות כלשהי, הוא יכול להעניק לעצמו את ההרשאה המבוקשת ללא בקרה מצד מנהל הרשת. הסיכון בכך הוא, שתחנת הקצה חשופה לכל פעולה שהתוקף יבחר לעשות.

מערכות ההפעלה יוצרות בדרך כלל באופן אוטומטי חשבון Admin, ולכן חשבון זה מוכר בקרב התוקפים ומהווה נקודת תורפה של הארגון.

חשוב לשים לב: לפני ביטול חשבון Admin יש לדאוג לשם משתמש אחר בעל הרשאות חזקות למקרה הצורך.

תהליך ההקשחה

ניתן לבטל את חשבון ה-Admin בכמה דרכים:

א. ידנית - בארגונים קטנים אפשר להגדיר עבור כל תחנת קצה שם משתמש חלופי עבור מנהל מקומי.

ב. על ידי הרצת script לאחר ההתקנה - https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.localaccounts/rename-localuser?view=powershell-5.1localuser?view=powershell-5.1

ג. באמצעות GPO.

2.6 "משתמש דבש" (Honey Pot) עקרון ההקשחה

"משתמש דבש" הינו משתמש פקטיבי, המוקם ברשת הארגונית עם פרטי משתמש פיקטיביים, שתפקידו לפתות תוקף פוטנציאלי לגשת ל"מלכודת דבש".[7]

תוקף שינסה לפרוץ לארגון, ינסה בדרך כלל לאתר כמה שיותר שמות משתמשים, על מנת להשיג "מבחר" של הרשאות חיבור לארגון - במטרה להגיע לשם משתמש עם הרשאות גבוהות. "משתמש דבש" נועד לטמון לתוקף מלכודת, אשר נפילתו לתוכה תעורר התרעה. על מנת שמשתמש זה יהיה אפקטיבי, אין לאפשר התחברות/הזדהות עם שם המשתמש הנ"ל, וכך - כשיבוצע ניסיון הזדהות, מיד תתקבל על כך התרעה, וניתן יהיה לדעת כמעט בוודאות שמדובר בניסיון חדירה לארגון.

תהליך ההקשחה

להלן פירוט צעדים שיש לבצע על מנת להגדיר "משתמש דבש":

- ראשית, יש ליצור שם משתמש "דבש" בעל שם אמין, אך לא לאפשר את החיבור עם שם המשתמש הנ"ל (וזאת באופן גורף).[8]
- יש ליצור משתמשי "דבש" לוקאליים ומשתמשים רשתיים (משתמשי דומיין).
- יש לדמות למשתמש "הדבש" את כלל ההרשאות הלגיטימיות בארגון, על מנת ששם המשתמש לא יעורר חשד בפני התוקף.
- יש להגדיר את שם משתמש "הדבש" בתוכנה המיועדת לאיתור שם משתמש מסוג "דבש", על מנת שהתוכנה תתריע על כך בעת חיבור.

שים לב!

1. שימוש ב"משתמש דבש" יכול לתרום לארגון בקיצור הזמן לאיתור מתקפה. זאת בתנאי שתוכנן נכון וכן קיים תהליך מעקב ותחזוקה לסביבת ה"מלכודת".

2. ככל שהארגון ישתמש ביותר שמות משתמשים מסוג "דבש" כך הוא מגדיל את הסבירות לזהות כי מתרחשת מתקפה.

[7] https://www.sans.edu/cyber-research/security-laboratory/article/honeypots-guide

[8] https://www.cse.wustl.edu/~jain/cse571-09/ftp/honey.pdf

3 הגנה על המידע

3.1 גיבוי המידע

עקרון ההקשחה

כאמור, תחנות הקצה בארגונים עלולות להכיל מידע רגיש רב, ולכן יכולות להיפגע מטעויות אנוש (מחיקה בשוגג של מידע) או בשל תקיפת סייבר. לדוגמה, אחת התקיפות הנפוצות ביותר הן כופרות - פוגענים אשר משביתים את המידע הקיים על תחנת הקצה באמצעות הצפנתו. התוקפים לא יאפשרו גישה למידע ללא תשלום הכופר. לעתים 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.[9]

תהליך ההקשחה

דרך ההתמודדות עם מתקפות מסוג כופרה היא גיבוי המידע באמצעי חיצוני - על גבי כונן רשת, כונן חיצוני או גיבוי בענן. חיבור האמצעי לתחנת הקצה ייעשה בזמן הגיבוי בלבד, ובשאר הזמן על אמצעי זה להיות מנותק באופן קבע מתחנת הקצה, כדי שלא ייפגע במקרה של חדירת פוגען.

דגשים חשובים:

- יש להקצות אמצעים פיזיים ייעודיים למטרת הגיבוי, כגון: שרת, ענן גיבוי, כונן רשת.
- יש להגדיר גורם אחראי על גיבוי המידע בארגון.
- יש להגדיר מדיניות של גיבוי מידע עיתי בארגון (יומי, שבועי, חודשי)
- יש לבצע בדיקת שחזור על מנת לוודא שהגיבוי אפקטיבי.

שים לב! גיבוי המידע יעזור לנו להתאושש במקרה שאבד מידע עסקי, ויתרום להמשכיות העסקית.

תורת הגנה בסייבר לארגון > המשכיות עסקית

3.2 מניעת דלף מידע (DLP)

עקרון ההקשחה

עובדים בארגון יכולים להוציא מידע רגיש אל מחוץ לארגון באמצעים שונים, כדוגמת: שליחה באמצעות מייל, העתקה להתקן USB ועוד.

הוצאת מידע רגיש יכולה להתרחש מכוונת זדון או כתוצאה מטעות אנוש. לכן שכבת אבטחה מפני זליגת מידע מהארגון היא בעלת חשיבות רבה. פתרונות מסוג DLP (Data Leak Prevention) מסייעים לארגון לבצע ניטור נתונים, ובהתאם למדיניות חוקים שנקבעה מראש - לחסום העברת מידע אל גורמים בלתי מורשים, ובכך למזער תקריות של אובדן מידע רגיש ודליפתו.[10]

כמו כן, מערכת DLP יכולה לתעד את פעולות המשתמש על תחנת הקצה ולבחון פעילות חשודה שיכולה להזיק לארגון, כגון מכירת מידע, ביצוע הונאות ופעולות זדוניות נוספות.

תהליך ההקשחה

הפעולות העיקריות שיש לבחון:

- 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.

[9] CIS Control 10 https://www.cisecurity.org/controls/data-recovery-capability.

[10] CIS Control 13 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 נוזקה/וירוס לכל מחשב המאפשר חיבור USB. כדי להגן על המידע הרגיש של הארגון **יש להגביל את הגישה לחיבור התקנים מסוג זה בנקודת הקצה.**

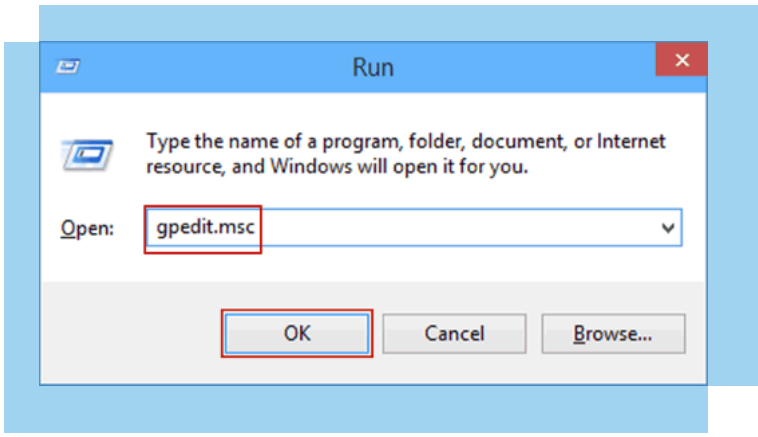
קיימות שתי נקודות תורפה בהן רצוי להגן על תחנת הקצה: הגנה על המחשב והגנה על ההתקנים הניידים שאנו משתמשים בהם.

תהליך ההקשחה

א. **הקשחת חיבור USB** בעזרת מערכת ההפעלה של המחשב:

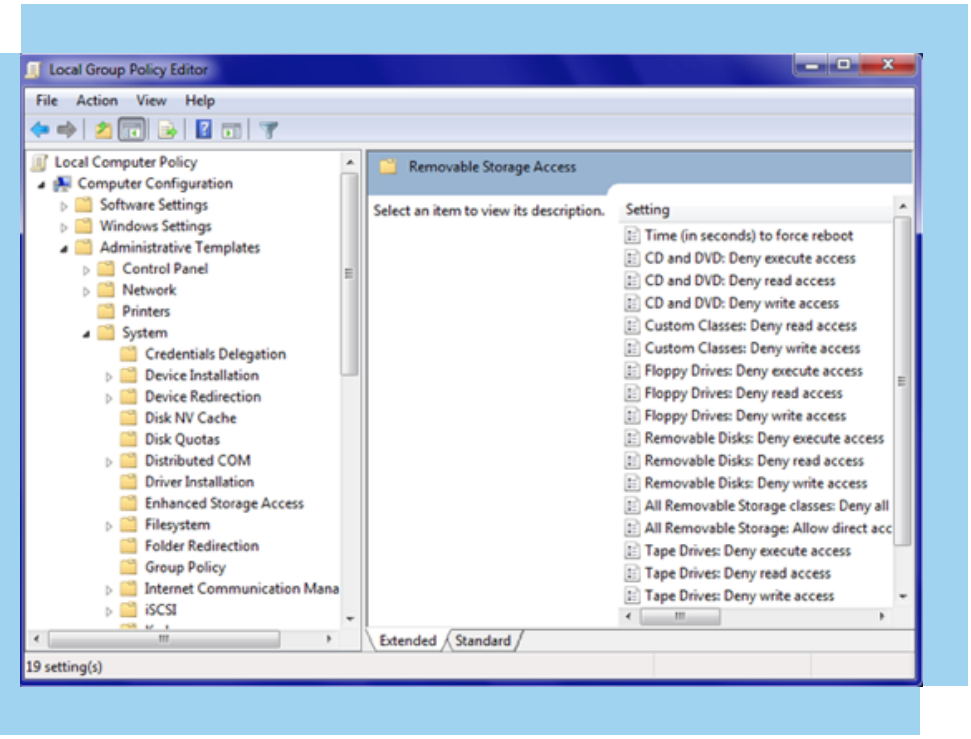
- ראשית יש ללחוץ על מקש "התחל" ולאחר מכן, בשורת החיפוש, יש להקליד: run.

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, ולאחר מכן יש לבחור באפשרות Removable Storage Access.

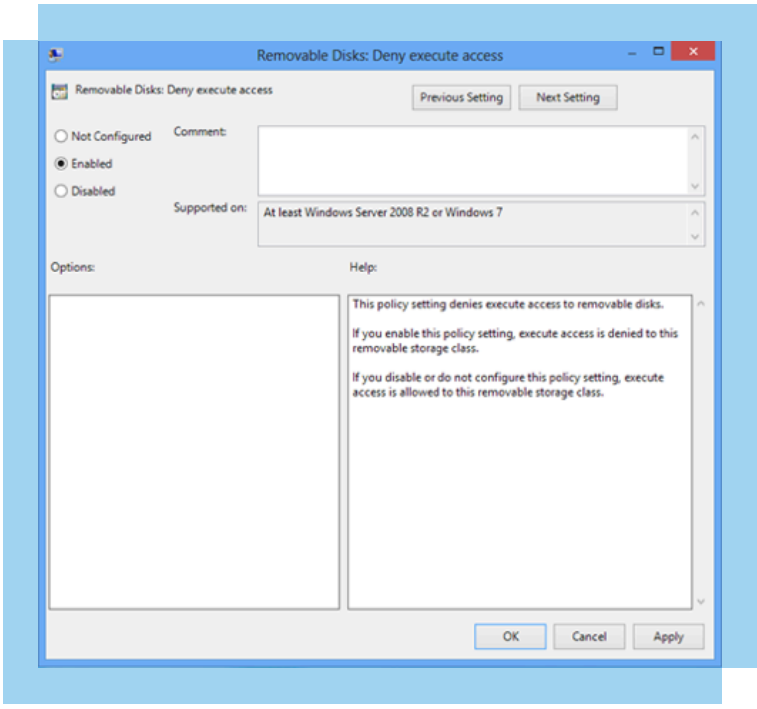


- כעת יופיעו 3 אפשרויות. יש לבחור בכל פעם באחת מהן על ידי לחיצה כפולה, ולסמן את האפשרויות האלה:

- Removable Disks : Deny execute access
- Removable Disks : Deny write access
- Removable Disks : Deny read access

שים לב! יש לבצע את סדר הפעולות הבא לכל אחת מ-3 האפשרויות.

- בחלון הבא יש לבחור באפשרות Enable, לאחר מכן ללחוץ על כפתור OK.



- בסיום יש לבצע אתחול.

ב. **הסרה פיזית:**

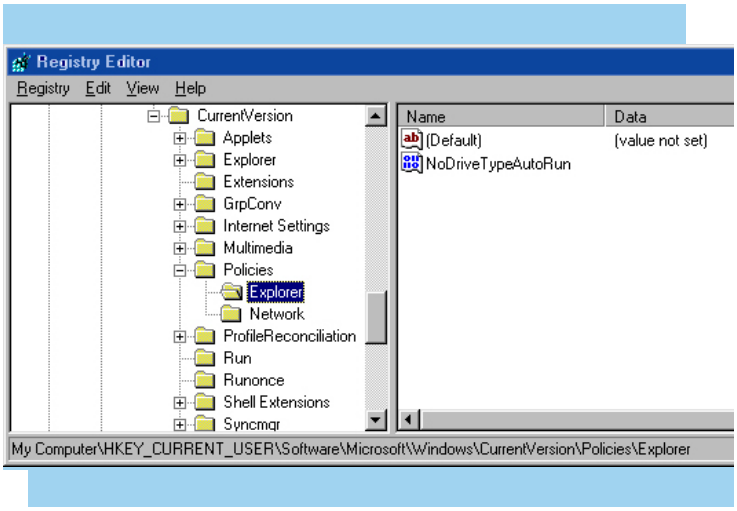
אפשרות אחרת היא **הסרה או חסימה פיזית של כונני דיסקים וכניסות USB.**[11]

ג. **הגנה על התקן נייד:**

Autorun - הגדרה זו מפעילה אוטומטית קבצים מהתקנים ניידים או פותחת תפריט אפשרויות. בפועל מכיל ההתקן קובץ שנקרא autorun.inf, שבו תוקפים עלולים "לשתול" פוגענים, אשר יופעלו באמצעות הרצה אוטומטית של כל הקבצים המפורטים בקובץ ה-Autorun.

לכן, חשוב להקשיח Autorun באופן הבא:

- ברשתות מבוססות דומיין Microsoft ניתן להגדיר ב-GPO חסימת התקנים.
- בנוסף, ניתן להקשיח מקומית את תחנת הקצה באופן הבא:
  - יש ללחוץ על שורת התחל ולאחר מכן בשורת החיפוש יש להקליד: run.
  - בחלון שנפתח יש לרשום regedit ולאחר מכן אישור.
  - יש לגשת לנתיב הבא:
    HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\NoDriveTypeAutorun



  - יש ללחוץ עם מקש העכבר הימני על האפשרות NoDriveTypeAutoRun ולאחר מכן לבחור באפשרות של Modify.
  - בשורת Value data יש לשנות את הערך ל-0xff, ולאחר מכן על אישור.
  - יש לאתחל את המחשב.

שים לב, שניתן לחסום רק חלק מהקבצים, לפי הטבלה המפורטת להלן:

[11] למעשה, אפשר לחסום באמצעים פיזיים כל ממשק לא נחוץ במחשב.

Value	Meaning
0x1 or 0x80	Disables AutoRun on drives of unknown type
0x4	Disables AutoRun on removable drives
0x8	Disables AutoRun on fixed drives
0x10	Disables AutoRun on network drives
0x20	Disables AutoRun on CD-ROM drives
0x40	Disables AutoRun on RAM disks
0xFF	Disables AutoRun on all kinds of drives

- **סריקת התקן נייד:**
מומלץ לבצע תמיד סריקה של התקן נייד לפני העתקה של קבצים ממנו או אליו, ובייחוד לפני הפעלה של קבצים ממנו. אם תוכנת האנטי-וירוס המותקנת בארגון מאפשרת זאת - מומלץ להגדיר סריקה אוטומטית של כל התקן נייד שמוכנס למחשב.

תורת הגנה בסייבר לארגון > אבטחת מדיה > 15.5

4 תוכנות אבטחה

4.1 אנטי-וירוס (Anti-Virus)[12]

עקרון ההקשחה

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

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 או בהתאם להמלצות היצרן).

הידעת?

"ארגז חול" (Sandbox) - כלי אמולציה שבאמצעותו האנטי-וירוס מנתח קובץ או תהליך במחשב, באזור הסגר בזיכרון. כאשר הווירוס נמצא באזור ההסגר, הוא אינו יכול להזיק וניתן לבדוק מה יהיו תוצאות הפעלתו בצורה מבודדת. אם הקובץ מתגלה כווירוס, האנטי-וירוס חוסם אותו ומודיע על כך למשתמש.
חתימת הקובץ - החתימה יכולה להיות חתימה סטטית, שהיא ערך גיבוב של פיסת קוד ייחודית לווירוס, או חתימה מבוססת התנהגות, דהיינו אם תוכנה מנסה לבצע פעולות כלשהן המוגדרות על ידי האנטי-וירוס כחשודות, עליו לעצור את פעולתה ולהודיע למשתמש.
בדיקה גנרית - האנטי-וירוס מנתח את התנהגותם של התהליכים הרצים במחשב, כולל מעקב אחר פעילותם, בדיקת ניסיונות גישה של תהליך לתהליכים אחרים, גישה למשאבים וכיוצא באלה. כשתהליך מסוים מתחיל לשנות קובץ מערכת, האנטי-וירוס מנטר את התנהגותו בקפידה.

[12] CIS Control 8 https://www.cisecurity.org/controls/malware-defenses.

4.2 מערכת EDR

עקרון ההקשחה

EDR (Endpoint Detection and Response) הוא מונח, המגדיר קטגוריה של כלים ופתרונות, המתמקדים באיתור המידע בתחנות הקצה בארגון ובניטורו. המערכת עובדת בעזרת סוכן, המותקן על תחנות הקצה. הסוכן בודק את האפשרות של מתקפות חיצוניות ושל איומים פנימיים, על ידי מעקב אחר תעבורת הרשת, פעילות בתחנת הקצה, הרצת שירותים ותהליכים ועוד. הסוכן אוסף את המידע הרלוונטי ושומר אותו במאגר מידע, שהוגדר לצורך כך מראש.

עובד אבטחת מידע שעובד עם המערכת יכול להשתמש במידע שנאסף לצורך זיהוי אנומליות, חקירה, דיווח והתראות על אירועי אבטחת מידע בארגון.

ייחודיות הפתרון היא בכך, שמדובר בפלטפורמה אחת אחודה, שמגינה על מחשבים ניידים, נייחים, שרתים ועל סביבות וירטואליות.

ניטור תחנות קצה וזמן תגובה קצר למתקפה מהווים מפתח לשמירה על תחנת קצה כמאובטחת.

פתרונות ה-EDR מסוגלים לאתר אירוע או איום סייבר ברשת על מספר רב של תחנות עבודה.

תהליך ההקשחה

יש לתכנן את מערכת ה- EDR באופן שיאתר את שרשרת האירועים ויאחסן אותם לצורך תחקור עתידי והשוואה לאירועים ברשת כדוגמת ניתוח התנהגותי. זאת בדגש על הגדרות שיאפשרו לאתר False positive ולמנוע אותם.

שים לב! פתרון EDR ינטר את הפעילויות בתחנות הקצה ויאפשר תחקור של אירועי אבטחת מידע.

תורת הגנה בסייבר לארגון > מניעת קוד זדוני > 7.8

Local Firewall 5

עקרון ההקשחה

מערכות הפעלה של תחנות קצה מספקות לרוב חומת-אש, המאפשרת לחסום תעבורה לא חוקית אל תחנת הקצה וממנה.[13]

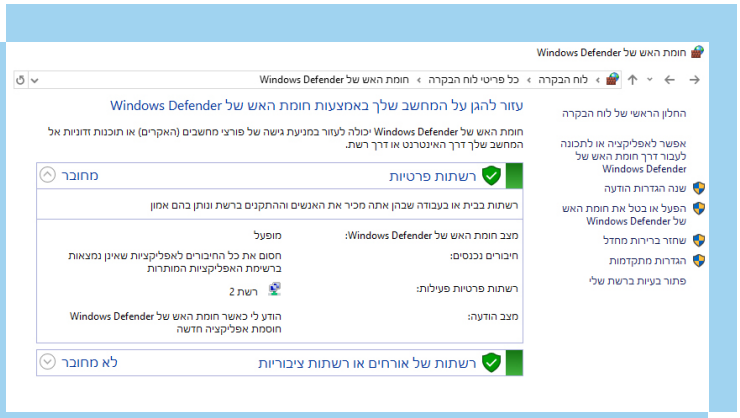
חומת-האש נועדה להגן על הרשת באמצעות זיהוי תעבורה שאינה מאושרת וחסימתה, ועוזרת לחסום תוכנות זדוניות, כגון וירוסים ופוגענים.

שים לב! חשוב להריץ את חומת-האש על תחנות הקצה גם אם ברשת הארגונית שלך כבר מותקנת חומת-אש ארגונית, מאחר שזוהי שכבת אבטחה נוספת.

תהליך ההקשחה

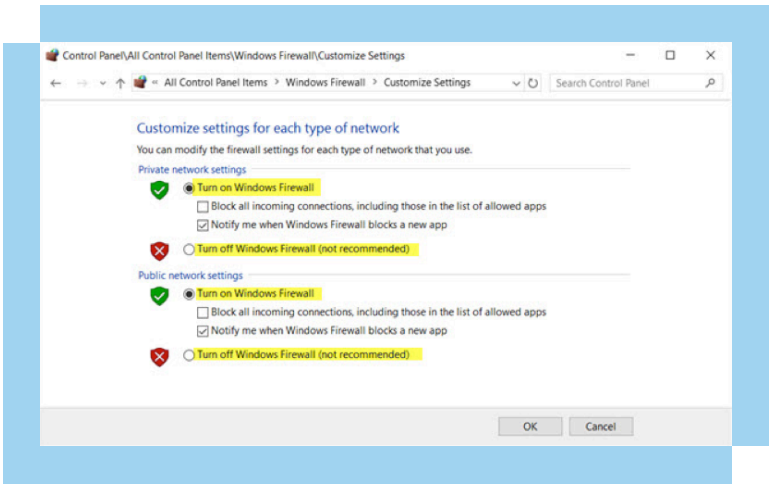
על מנת לוודא שחומת-האש אכן רצה ברקע, יש לפעול על פי סדר הפעולות הבא:

- יש ללחוץ על "התחל" ולאחר מכן לבחור באפשרות של לוח בקרה. לאחר מכן יש לבחור באפשרות Windows Firewall.



[13] CIS Control 9 https://www.cisecurity.org/controls/limitation-and-control-of-network-ports-protocols-and-services

• לוודא שהאפשרות שנבחרה היא: Turn Windows Firewall On מצד שמאל של המסך. יש לוודא ששתי האפשרויות מסומנות כמו בתצלום הבא:



תורת הגנה בסייבר לארגון < הגנת תחנות עבודה ושרתים < **6.1**

• ל-Windows FW יש שלושה פרופילים לסביבות שונות: PRIVATE, PUBLIC ו-DOMAIN. למידע נוסף: https://msdn.microsoft.com/enus/library/windows/desktop/bb736287(v=vs.85).aspx

6 עדכוני אבטחה

עקרון ההקשחה

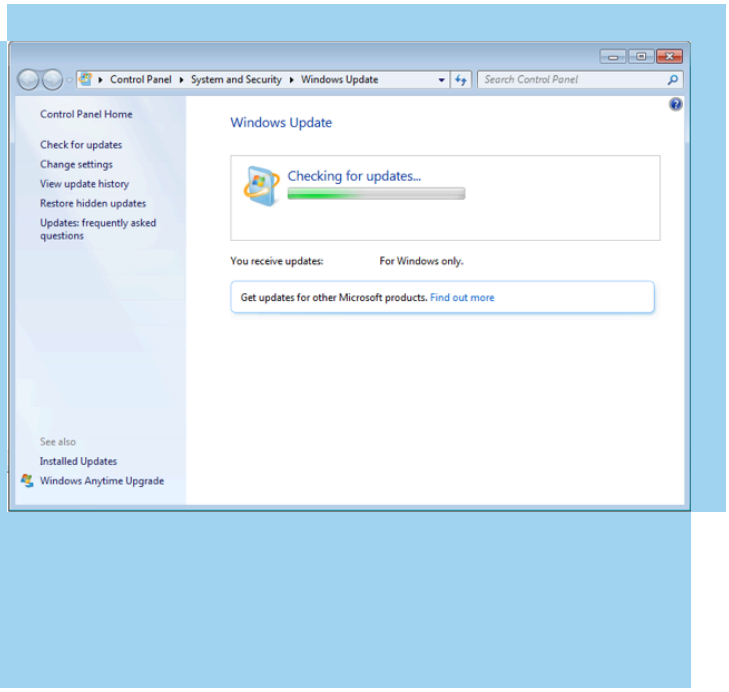
בכל תוכנה מתגלים לעתים כשלים, שהתוקפים עלולים לנצלם לתקיפת תחנת הקצה. מרבית יצרני התוכנות מספקים עדכוני אבטחה למוצריהם על מנת לסייע ללקוחותיהם לשמור על תחנות הקצה מוגנות. בפרט יצרני מערכות הפעלה, שהן רכיב התוכנה המרכזי בכל תחנת קצה, מספקים עדכוני אבטחה על בסיס קבוע (בדרך כלל פעם בחודש) ולעתים מפיצים עדכונים קריטיים בתדירות גבוהה אף יותר. **ביצוע עדכונים באופן שוטף ממזער את האפשרות שתוקף ינצל חולשות אלו.**[14]

תהליך ההקשחה

ככלל, 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.

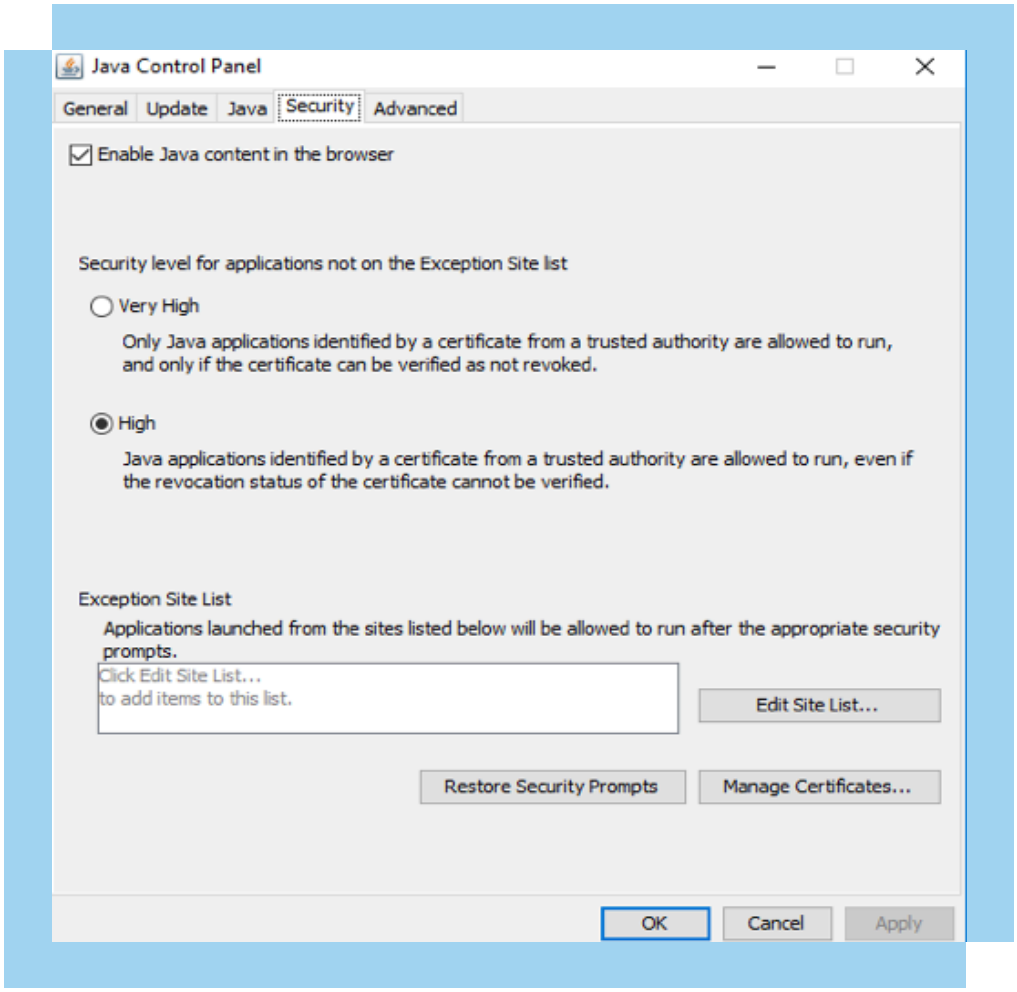
יש לבצע את הפעולות הבאות:

• יש ללחוץ על "התחל" > בלוח הבקרה בשורת החיפוש להקליד Windows updates.



[14] CIS Control 3 https://www.cisecurity.org/controls/continuous-vulnerability-management.

- יש לבחור באפשרות Check for updates.



שים לב! יש לבצע באופן שוטף עדכונים לתחנות הקצה על מנת למנוע מתוקפים לנצל פרצות אלו.

תורת הגנה בסייבר לארגון > מניעת קוד זדוני > 7.9

נספח א'

רשימת תיוג מומלצת

נושא	בוצע	חלקי	לא בוצע
אבטחה פיזית של תחנות קצה	☐	☐	☐
הקשחת BIOS	☐	☐	☐
הצפנת דיסק קשיח	☐	☐	☐
הפחתת חשבונות admin	☐	☐	☐
מדיניות סיסמאות	☐	☐	☐
ביטול Local Admin	☐	☐	☐
התקנת "מלכודות דבש"	☐	☐	☐
גיבוי מידע	☐	☐	☐
מניעת דלף מידע	☐	☐	☐
חסימת התקנים	☐	☐	☐
התקנת אנטי-וירוס	☐	☐	☐
התקנת מערכת EDR	☐	☐	☐
הפעלת חומת-אש מקומית	☐	☐	☐
הפעלת עדכוני אבטחה	☐	☐	☐

סייבר ישראל
משרד ראש הממשלה
מערך הסייבר הלאומי

*9344
tora@cyber.gov.il
www.cyber.gov.il
חפשו אותנו