נהלי אבטחת מידע – הקשחות מומלצות	

הקשחת מערכות מחשוב

דרכי פעולה מומלצות
(Best Practices)

1.הקדמה

משטח התקיפה (Attack Surface) במרחב הסייבר מייצג את כלל הממשקים דרכם יריב (Adversary) פוטנציאלי עשוי לבצע תהליך התערבות אינטראקציה לא רצוי עם מערכת המחשוב. דוגמא לחדירה לצורך שיבוש הינה הזנת קלט (Input) זדוני ע״י יריב לממשק מבוסס תוכנה וזאת במטרה לפגוע בתקינות פעילות מערכת המחשוב או השגת גישה למידע רגיש/חסוי המאוחסן במערכת המחשוב ע״י יריב.

צמצום משטח התקיפה מהווה אמצעי אפקטיבי המקשה על יריבים במרחב הסייבר להגשים את תכליתם, דבר אשר משפר את כושר עמידות הארגון בפני תקיפות סייבר.

אחת מן השיטות המקובלות לצמצום משטח התקיפה הינה הקשחה (Hardening), הכוללת ביצוע שינויים בפרמטרי הפעלה/קונפיגורציה (Configurations) של מערכת המחשוב. דוגמא שכיחה להקשחה הינה חסימה של הפעלת שירותי מערכת (System Services) שאינם נדרשים לפעילות בשגרה או שינוי סף הפעולה (Threshold) של מנגנון אבטחה.

2.מטרת המסמך

מטרת המסמך הינה לסייע לארגון לצמצם את משטח התקיפה, וזאת על ידי ביצוע פעולות ובקרות להקשחת מערכות המחשוב הקיימות בארגון.

3. קהל היעד למסמך

קהל היעד העיקרי של מסמך זה הוא מנהל הגנת הסייבר (CISO), ארכיטקטי הגנה בסייבר/טכנולוג הגנה בסייבר (Cyber Security Technology Professional), מומחה מתודולוגיות הגנת סייבר (Cyber Security Methodology Professional), מיישמי סייבר (Cyber Security Practitioners) וצוותי הסיסטם.

נהלי אבטחת מידע – הקשחות מומלצות	

4.שלבי העבודה

סביבת העבודה המודרנית נסמכת על קיומה של תשתית מחשוב המבוססת על ממשקים המאפשרים החלפת מיידעים ו/או פקודות הפעלה בין :

א. מודולים המובנים במערכת מחשוב

ב. מערכת מחשוב אחת למשניה

ג. משתמש אנושי למערכת המחשוב

ממשקים אלו יוצרים את משטח התקיפה (Surface Attack), אשר יריב עשוי לנצלם לשם השגת תכליתו.

השליטה על ממשקים אלו מבוססת על ביצוע שינויים בפרמטרי הפעלה/קונפיגורציה, (Configurations) כאשר חלק ניכר משינויים אלו ניתנים להחלה ברמת תוכנה.

בעולם מקובלות מספר מתודולוגיות לביצוע הקשחה, כאשר המובילות שבהן הינן מבית סוכנות התקשוב של משרד ההגנה האמריקאי (Defense Information Systems Agency) , והאחרת פרי הארגון הבינלאומי (ארגון ללא מטרות רווח) מרכז האבטחה לאינטרנט (Center for Internet Security). כמו כן, חלק מהיצרנים מפרסמים מעת לעת הנחיות לביצוע הקשחה, אם כי תדירות הפרסום אינה קבועה במרבית המקרים, ואף לעיתים המשתמש/בעל הצורך נדרש לאתר מספר רב של מסמכים לשם בניית סט ההנחיות המלא הנדרש להחלה.

כל מתודולוגיה מציעה סט של הגדרות להחלה, וזאת בהתאם למדרג חומרה (Level Severity) וסוג/גרסה של נכס הסייבר (Cyber-Asset) הרלוונטי.

שיטת החלת מתודולוגיית הקשחה כוללת מספר שלבים עיקריים :

תרשים 1: שלבים עיקריים בהחלת מתודולוגיית הטמעה

נהלי אבטחת מידע – הקשחות מומלצות	

מס׳	שם השלב	הסבר משלים	דוגמא לתוצר
.1	זיהוי נכס הסייבר ומאפייניו	זיהוי נכס הסייבר ומאפייניו, כדוגמת: תפקיד נכס הסייבר, שם היצרן, מהדורה, גרסה.	שרת מסד נתונים תוצרת חברת XYZ מהדורת Enterprise, גרסת 2019.
.2	איתור הנחיות לביצוע הקשחה	גישה לאתר יצרן המתודולוגיה, והורדת התיעוד לביצוע הקשחה (לרבות סקריפטים או עזרים אחרים) המתאימות לנכס הסייבר אשר זוהה בשלב הקודם.	גישה לאתר יצרן המתודולוגיה (כדוגמת DISA STIG1), והורדת התיעוד ועזרים.
.3	החלת עקרון פונקציונאליות נמוכה	הסרה של פונקציונאליות שאינה נדרשת לעבודה שוטפת בנכס הסייבר.	הסרת פרוטוקול SMB 1.0.
.4	בחירה במדרג החומרה להקשחה	עיון בתיעוד המתייחס למדרגי החומרה להקשחה, ובחירה של מדרג בהתאם למתאר האיומים.	המלצת מערך הסייבר הלאומי הינה להשתמש ברמת חומרה מסוג DISA Categories I + II 2 לכל הפחות.
.5	בדיקות תאימות בסביבת בדיקות	החלת ההקשחה בסביבת בדיקות ייעודית של נכס הסייבר המדמה פעילות ייצור, וזאת על-מנת לוודא כי הסבירות לפגיעה בזמינות תפעולית לאחר ביצוע ההקשחה הינה נמוכה. במקרה של איתור מגבלה, יש לבחון האם נדרש לבצע עדכון להנחיות ההקשחה ו/או ליישום אשר בו אותרה המגבלה.	מערכת ההפעלה של עמדות הקצה עברה הקשחה; א. ההקשחה עברה בהצלחה, ולא אותרה מגבלה תפעולית. ב. עקב מגבלות אפליקטיביות הוחלט לקבל את הסיכון, ולמנוע החלה של דרישת אבטחה פלונית.

נהלי אבטחת מידע – הקשחות מומלצות	

מס׳	שם השלב	הסבר משלים	דוגמא לתוצר
6.	בחינת יכולת חזרה לאחור (Rollback)	בחינת יכולת חזרה לאחור – למצב לפני הקשחה, וזאת על-מנת לוודא שבמקרה של תקלה בסביבת הייצור, ניתן יהיה לחזור למצב עבודה תקין.	בניית תוכנית חזרה לאחור, ובחינת האפקטיביות שלה ביחס לסביבת העבודה בארגון.
7.	בדיקות תאימות בסביבת יצור	החלה בדיקות על מספר מדגם מייצג של נכסי סייבר בסביבת יצור, וזאת על-מנת לוודא כי הסבירות לפגיעה בזמינות תפעולית לאחר ביצוע ההקשחה הינה נמוכה. במקרה של איתור מגבלה, יש לבחון האם נדרש לבצע עדכון להנחיות ההקשחה ו/או למערכת המחשוב אשר המגבלה מתייחסת אליה.	מערכת ההפעלה של עמדות הקצה עברה הקשחה ; א. ההקשחה עברה בהצלחה, ולא אותרה מגבלה תפעולית. ב. עקב מגבלות אפליקטיביות הוחלט לקבל את הסיכון, ולמנוע החלה של דרישת אבטחה פלונית.
8.	החלת ההקשחה בסביבת הייצור	החלת ההקשחה בסביבת הייצור באופן מדורג, בין אם ע״י החלה ברמת ה- Golden Image או באמצעות שיטה אחרת.	מערכת ההפעלה של עמדות הקצה עברה הקשחה לפי אחוזי פריסה 10, 25, 40, 50, 75, 100%
9.	בדיקת רציפה של רמת ציות/תאימות (Compliance)	בדיקת רציפה של רמת ציות, וזאת על-מנת לוודא כי ההקשחה אפקטיבית וישימה. במקרה של חריגה, יש לוודא החלה מחדש של ההקשחה.	ביצוע בדיקת לקיום ההקשחה ע״י תוכנה ממוכנת לאיתור חולשות Vulnerability Assessment התומכת במתודולוגיית ההקשחה (כדוגמת DISA) ופרוטוקול/תקן SCAP (Security Content Automation Protocol).

נהלי אבטחת מידע – הקשחות מומלצות	

מס׳	שם השלב	הסבר משלים	דוגמא לתוצר
.10	בחינת עדכניות ההקשחה	בחינת עדכניות ההקשחה בהתאם לגרסאות המומלצות ע״י יצרן מתודולוגיה ההקשחה, ובהתאם לגרסאות/מהדורות מערכות המחשוב בארגון.	רישום לרשימת תפוצה הכוללת עדכונים אודות מתודולוגיית ההקשחה. להלן שתי דוגמאות: א. מתודולוגית ההקשחה אשר הוטמעה בעבר למערכת הפעלה פלונית הינה Ver 2, 12 Release. יצרן המתודולוגיה פרסם Ver 3, Release 1, ולפיכך עולה הצורך להחיל את ההקשחה החדשה בהתאם. ב. למערכת הפעלה פלונית יצא עדכון תוכנה המשנה את גרסת המוצר (Build Number), ולפיכך נדרש להבטיח תאימות מול מתודולוגיית ההקשחה המומלצת.

טבלה 1: שלבי העבודה העיקריים להטמעת מתודולוגית הקשחה

נהלי אבטחת מידע – הקשחות מומלצות	

להלן דוגמה למיפוי משפחות נכסי סייבר, ביחס למדרג חומרה להקשחה מומלץ)לרבות הפנייה למקור מתודולוגיית ההקשחה(:

מס'	משפחת פתרונות	מדרג חומרה להקשחה מומלץ	מקור ההקשחה
.1	מערכות הפעלה פתרונות וירטואליזציה שרתי אינטרנט (Web) שרתי דוא"ל (email) שרתי מסדי נתונים (Database) ציוד תקשורת	DISA STIG Categories/levels 1+2	https://public.cyber.mil/stigs/downloads/ או https://public.cyber.mil/stigs/ או https://public.cyber.mil/stigs/gpo/
.2	תוכנות משרדיות	DISA STIG Categories/levels 1+2 או המלצות יצרן	https://public.cyber.mil/stigs/downloads/ או https://public.cyber.mil/stigs/ או https://public.cyber.mil/stigs/gpo/ או אתר האינטרנט של יצרן הפתרון ו/או קבלת המלצות פרטניות מצוות התמיכה של היצרן

נהלי אבטחת מידע – הקשחות מומלצות	

מס'	משפחת פתרונות	מדרג חומרה להקשחה מומלץ	מקור ההקשחה
.3	מדפסות	DISA STIG Categories/levels 1+2 או המלצות יצרן	https://public.cyber.mil/stigs/downloads/ או https://public.cyber.mil/stigs/ או אתר האינטרנט של יצרן הפתרון ו/או קבלת המלצות פרטניות מצוות התמיכה של היצרן
.4	מערכי אחסון מערך גיבוי שירותי ענן ציבוריים מערך אבטחת מידע	המלצות יצרן	אתר האינטרנט של יצרן הפתרון ו/או קבלת המלצות פרטניות מצוות התמיכה של היצרן

טבלה 2: שלבי העבודה העיקריים להטמעת מתודולוגית ההקשחה

נספח א – הבדלים עקרוניים בין קטגוריות.5

נהלי אבטחת מידע – הקשחות מומלצות	

ההקשחה השכיחות ב-DISA STIG

להלן רשימת קטגוריות ההקשחה השכיחות ב-DISA STIG. כל קטגוריה קובעת סט דרישות הקשחה להחלה בהתאם למתאר האיום. ככלל, המלצת מערך הסייבר הלאומי הינה להחיל את דרישות הקשחה המופיעות תחת קטגוריות I + II , לכל הפחות.

Category I	Category II	Category III
כל חולשה אשר ניצול (Exploit) שלה יגרום באופן ישיר ומידי לפגיעה בסודיות (Confidentiality), זמינות (Availability) או מהימנות ושלמות (Integrity).	כל חולשה אשר ניצול שלה יוצר פוטנציאל לפגיעה בסודיות, זמינות או מהימנות ושלמות.	כל חולשה אשר קיומה פוגע ביכולת להגן מפני פגיעה בסודיות, זמינות או מהימנות ושלמות.

מדרג חומרת החולשה

טבלה 3: הבדלים עקרוניים בין קטגוריות ההקשחה השכיחות ב-DISA STIG

6.קיצורי שמות

פרק זה מציג ביאור לקיצורי השמות בהם נעשה שימוש במסמך זה.

מס'	קיצור שם	ביאור
.1	API	Application Programming Interface
.2	CIS	Center for Internet Security
.3	DevOps	Software Development (Dev) and Information Technology Operations (Ops)
.4	DISA	Defense Information Systems Agency
.5	NIST	National Institute of Standards and Technology
.6	PCI	Payment Card Industry
.7	QA	Quality Assurance
.8	SCAP	Security Content Automation Protocol
.9	SMB	Server Message Block
.10	SP	Special Publishing
.11	STIG	Security Technical Implementation Guide

טבלה 4: קיצורי שמות

7.מסמכים ישימים

CIS Benchmarks - Center for Internet Security

CIS Benchmarks. Center for Internet Security (CIS). (n.d.). Retrieved from http://www.cisecurity.org/cis-benchmarks/

DISA

Group Policy Objects. DoD Cyber Exchange. (2021, November 12). Retrieved from https://public.cyber.mil/stigs/gpo/

Security Technical Implementation Guides (STIGs). DoD Cyber Exchange. (n.d.). Retrieved from https://public.cyber.mil/stigs/

Stigs Document Library. DoD Cyber Exchange. (n.d.). Retrieved from https://public.cyber.mil/stigs/downloads/

NIST

Quinn, S. D., Souppaya, M., Cook, M., & Scarfone, K. (2018, February). *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf

Scarfone, K., Jansen, W., & Tracy, M. (2008, July). *Guide to General Server Security*. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

PCI

Payment Card Industry (PCI) Data Security Standard. PCI Security Standards Council. (2018, May). Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf