סייבר ישראל
מערך הסייבר הלאומי

המלצות ליישום
(Best Practices)
אבטחת העברה מנוהלת של קבצים (MFT)

סייבר ישראל
מערך הסייבר הלאומי

המלצות ליישום
(Best Practices)

אבטחת העברה מנוהלת של קבצים (MFT)

ינואר 2021

תוכן עניינים

אבטחת העברה מנוהלת של קבצים (MFT)

1. מבוא (Introduction)

1.1 כללי

ארגונים במשק נדרשים לקבל או לשלוח קבצים על בסיס של קבע לשותפים עסקיים וגורמים אחרים תוך שימוש בתשתית תקשורת ציבורית, דוגמת רשת האינטרנט. המידע המועבר בקבצים עשוי לכלול מידע פיננסי של הארגון ולקוחותיו, דיווחי שעות עבודה של עובדי הארגון הנשלחים לחברות המתמחות בתחום, קבצי גיבויים המועברים לאחסון בגורם צד-שלישי או באתר אחר של הארגון ועוד.

המימוש הטכנולוגי המקובל כולל שימוש במערכת להעברה מנוהלת של קבצים (MFT – Managed File Transfer), כאשר אחד הפתרונות המסורתיים הינו "כספות" (Vaults).

1.2 מודלים מקובלים להטמעה

מקובל לראות כי פתרונות ה-MFT הזמינים בשוק עושים שימוש במספר מודלים להטמעה:

מס'	תצורת עבודה	גורם אחראי	מיקום המערכת	גורם מתפעל	מיקום אחסון הקבצים
1.	עבודה מקומית (On Premise)	הארגון	בארגון	הארגון	בצד המקבל או השולח
2.	עבודה היברידית (Hybrid)	אחריות משותפת (Shared Responsibility)	בארגון ובספק חיצוני	הארגון וספק חיצוני	בצד המקבל או השולח, ובספק ענן
3.	עבודה בענן (SaaS)	אחריות משותפת	ספק חיצוני	ספק חיצוני	בצד המקבל או השולח, ובספק ענן

טבלה 1: מודלים להטמעת מערכת MFT

ההחלטה מהו מודל ההטמעה הרצוי עשויה להיגזר מדרישות עסקיות ואילוצים שונים (דוגמת זמינות כוח אדם), דבר המחייב את הארגון לבצע התאמה של בקרות ההגנה לפרופיל הסיכון. כך לדוגמא, בעת עבודה עם ספק ענן

הארגון יידרש לבחון את ההשלכות הנגזרות מתצורת עבודה זו, לרבות עיגון חלק ניכר מבקרות ההגנה כחלק מחוזה ההתקשרות, וזאת תוך ביצוע בדיקות חוסן עיתיות או הסתמכות על דו"חות גורמי צד-שלישי.

1.3 מימושים טכנולוגים שכיחים למערכת MFT

ניתן למצוא בשוק מספר מימושים טכנולוגיים שכיחים למערכות MFT:

מס'	המימוש הטכנולוגי	תיאור	שיטת הזדהות	הצפנת תהליך העברת פקודות	הצפנת תהליך העברת נתונים	הצפנה של מסר בודד	חתימה דיגיטלית של מסר בודד	הערות
.1	FTP	העברת קבצים באמצעות פרוטוקול FTP.	שם משתמש + סיסמה	לא	לא	לא	לא	
.2	FTPS	העברת קבצים באמצעות פרוטוקול FTP על-גבי תווך מוצפן.	שם משתמש + סיסמה תעודה דיגיטלית שילוב של הנ"ל	כן	כן	לא	לא	מחייב פתיחה של מספר רב של פורטים ב-FW
.3	SFTP	העברת קבצים באמצעות פרוטוקול SSH	שם משתמש + סיסמה תעודה דיגיטלית (SSH keys) שילוב של הנ"ל	כן	כן	לא	לא	עושה שימוש בפורט אחד בלבד
.4	כספות (Vaults)	העברת קבצים באמצעות פרוטוקול ייעודי	שם משתמש + סיסמה	כן	כן	כן	כן	

			תעודה דיגיטלית (SSH keys) שילוב של הנ"ל הספק עשוי להציע שיטות הזדהות נוספות					
.5	דוא"ל מאובטח (Secure Mail)	העברת קבצים באמצעות ממשק דוא"ל. שכיח כי ניתן לבצע הצפנה ברמת התוכן ו/או ברמת המסר הבודד.	שם משתמש + סיסמה תעודה דיגיטלית (SSH keys) שילוב של הנ"ל הספק עשוי להציע שיטות הזדהות נוספות	כן	כן	כן	כן	
.6	שירות קבצים בענן ציבורי (SaaS)	העברת קבצים באמצעות ממשק אשר ספק הענן מציע ללקוחות	שם משתמש + סיסמה Access keys SAS - Shared Access Signature תעודה דיגיטלית שילוב של הנ"ל	כן	כן	תלוי מקרה	תלוי מקרה	ספק הענן עשוי להציע מגוון שירותי אחסון (דוגמת Object Storage, Table storage, Queue storage, File (storage

		הספק עשוי להציע שיטות הזדהות נוספות							

טבלה 2: מימושים טכנולוגים שכיחים למערכת MFT

מומלץ כי ארגונים אשר מעוניינים לעשות שימוש בשירות ענן ציבורי יבחנו היטב את יכולות ההגנה בסייבר המובנות בפתרון, וזאת תוך הכרת המגבלות המובנות. לדוגמא, השימוש ב- SAS URI מאפשר להגדיר אורך חיים מקסימלי למידע, שלאחריו הגישה מוסרת אוטומטית. עם זאת, ההשלכות הנגזרות במקרה של אובדן/גניבת פרטי ה-SAS והצעדים הנדרשים להתמודדות עם אירוע סייבר עשויים להיות שונים משמעותית בין ספק ענן אחד למשנהו, ואף בין שירות אחסון אחד למשנהו של אותו ספק ענן.

1.4 תהליך רישום המשתמשים (Onboarding\Enrolment)

תהליך רישום המשתמשים (Onboarding\Enrolment) מהווה צומת קריטית ראשונה, אשר נדרש לוודא את עמידותה בפני תקיפות סייבר.

ככלל, מומלץ כי שלב הרישום יתבצע שלא בצורה ישירה מול מערכת ה-MFT, אלא לאחר הרשמה מול "אזור אישי" או הזדהות חזקה מול מערכת הזדהות ייעודית אחרת.

להרחבה בנושא מומלץ לעיין ב"מדיניות לאומית להזדהות בטוחה[1]" מטעם מערך הסייבר הלאומי.

1.5 תהליך אימות המשתמשים (Authentication)

תהליך אימות המשתמשים (Authentication) מהווה צומת קריטית שנייה, אשר נדרש לוודא את עמידותה בפני תקיפות סייבר.

ניתן לחלק את המשתמשים לשלוש ישויות עיקריות:

א. משתמשים פנים ארגוניים בעלי הרשאות ניהול

ב. משתמשים פנים ארגוניים בעלי הרשאות גישה לכספת

ג. משתמשים חיצוניים לארגון בעלי הרשאות גישה לכספת

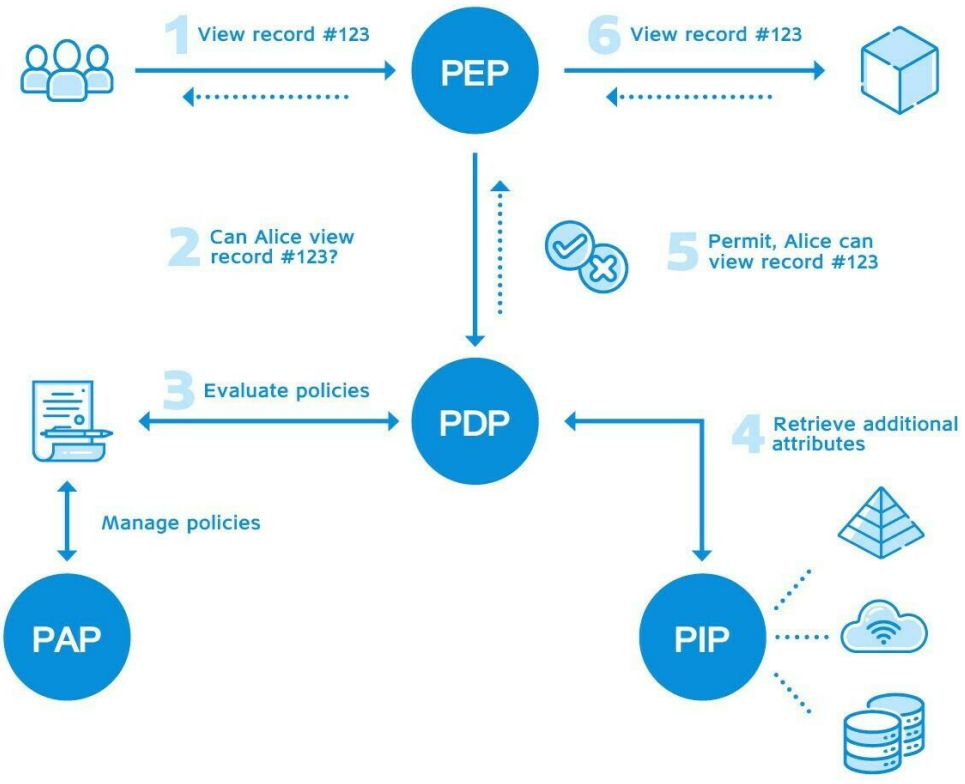
[1] מדיניות לאומית להזדהות בטוחה
https://www.gov.il/he/departments/news/bio_safeidpolicy

מקובל כי תהליך אימות משתמשים פנים ארגוניים מסתמך על שימוש בפרוטוקול Kerberos או על פרוטוקול אחר מול שירותי הספרייה הארגונית (Directory Services). כמו כן, שכיח כי לטובת אימות משתמשים חיצוניים לארגון נעשה שימוש בפרוטוקולים דוגמת OpenID Connect או SMAL 2.0 (מסורתי יותר, ונחשב לפחות גמיש כיום). ראוי לציין כי היתרון המהותי של השימוש בפרוטוקולים אלו הינו רמת התאימות הגבוהה לעבודה בתצורת פדרציה (Federation) מול ספקי ענן או גורמי צד-שלישי. ראוי לציין כי תהליך האימות עשוי לכלול אינטראקציית שרות ניהול זהויות בענן (IAM - Identity and Access Management).

1.6 בקרת גישה / ניהול הרשאות (Authorization)

בקרת הגישה במערכת ה-MFT מהווה צומת קריטית שלישית, אשר נדרש לוודא את עמידותה בפני תקיפות סייבר.

תקן RFC 2904[2] מציע מסגרת מקובלת לניהול בקרת גישה (Authorization). התרשים הבא סוקר את הרכיבים העיקריים המעורבים בתהליך ניהול הרשאות גישה.



תרשים 1: תהליך בקרת גישה לפי RFC 2904

[2] AAA Authorization Framework
https://tools.ietf.org/html/rfc2904

להלן סקירה של הרכיבים העיקריים המעורבים בתהליך ניהול הרשאות גישה:

מס'	תפקיד	תיאור
.1	נקודת ניהול מדיניות (PAP - Policy Administration Point)	רכיב המנהל את מדיניות הרשאות הגישה (Authorization)
.2	נקודת החלטת מדיניות (PDP - Policy Decision Point)	רכיב הבוחן את בקשת הגישה למשאב ביחס להרשאה קיימת או לא קיימת
.3	נקודת אכיפת מדיניות (PEP - Policy Enforcement Point)	רכיב האוכף את המדיניות בהתאם להחלטת ה-PDP. כלומר הגישה למשאב מאושרת או נדחית ברכיב זה, וזאת על סמך החלטת PDP.
.4	נקודת מידע על מדיניות (PIP - Policy Information Point)	רכיב המאחסן תכונות אובייקטים (סכמה), דוגמת משאב, נושא, סביבה.
.5	נקודת אחזור מדיניות (PRP - Policy Retrieval Point)	רכיב המאחסן את מדיניות הרשאות הגישה העושה שימוש בשפה הצהרתית מקובלת (דוגמת XACML). לטובת האחסון בדרך כלל נעשה שימוש במערכת קבצים או מסד נתונים. במקרים מסוימים תיתכן אינטראקציה עם שירותי הספרייה הארגונית (Directory Services).

טבלה 3: רכיבים עיקריים המעורבים בתהליך בקרת גישה

להלן סקירה של השלבים העיקריים בבחינת בקשת גישה מצד משתמש:

מס'	תיאור שלב הפעולה
.1	המשתמש שולח ל-PEP בקשה לקבלת גישה.
.2	ה-PEP ממיר את בקשת המשתמש לפורמט מקובל לבקשת גישה (דוגמת XACML).

3.	ה-PEP מעביר את הבקשה לבחינת ה-PDP.
4.	ה-PDP בוחן מהי המדיניות הרלוונטית לבקשה, ומתשאל את ה-PRP לשם קבלת המדיניות (וחוקי הגישה הרלוונטיים). ראוי לציין כי ה-PAP מאפשר ניהול של מדיניות ה-PRP. כמו כן, במקרי הצורך מתבצעת פנייה ל-PIP לקבלת מידע אודות תכונות רלוונטיות של האובייקטים.
5.	ה-PDP מקבל החלטה האם לאשר או לדחות את בקשת המשתמש, וה-PEP מבצע אכיפה של ההחלטה.

טבלה 4: השלבים העיקריים בבחינת בקשת גישה של משתמש

מקובל כי בשלב זה נעשה שימוש בטוקני ניהול הרשאות מקובלים דוגמת OAuth2 או SMAL 2.0 (מסורתי יותר, ונחשב לפחות גמיש כיום).

1.7 ארכיטקטורה מאובטחת ליישום מערכת להעברה מנוהלת של קבצים

ניתן להטמיע את מערכת ה-MFT בתצורות שונות, וזאת תוך החלת הפרדה לוגית או פיזית בין ערוץ הוצאת קבצים מהארגון, לבין ערוץ הכנסת קבצים לארגון.

להלן מצ"ב ארכיטקטורה טיפוסית ובסיסית לערוץ הוצאת קבצים מהארגון הכוללת יישום אמצעי אבטחה רשתיים מקובלים.

תרשים 2: ערוץ הוצאת קבצים מהארגון

להלן מצ"ב ארכיטקטורה טיפוסית ובסיסית לערוץ הכנסת קבצים לארגון הכוללת יישום אמצעי אבטחה רשתיים מקובלים.

תרשים 3: ערוץ קבלת קבצים מחוץ לארגון

תצורת העבודה הכוללת שימוש בשרת קדמי (Frontend) ושרת אחורי (Backend) מאפשרת להקטין את משטח התקיפה (Attack Surface) הפוטנציאלי. ובמילים אחרות, לאור העובדה כי השרת הקדמי לא אמור להחזיק מידע לאחר העברתו ליעד, גם אם תוקף אשר השיג שליטה מלאה על שרת היעד, ניתן לצמצם משמעותית את יכולתו לנצל את האחיזה לרעה.

ארגונים המעוניינים להשיג רמת אבטחה גבוהה עשויים להעדיף לעשות שימוש בבודל חד-כיווני (Data-Diode).

2. מטרות ויעדים (Goals & Objectives)

מסמך זה מציג המלצות ליישום לשם אבטחת העברה מנוהלת של קבצים (MFT).

3. קהל היעד (Target Audience)

מסמך זה נכתב עבור מנהל הגנת הסייבר בארגון (CISO), מסמך מתודולוגיות הגנת סייבר, מסמך מיישם הגנת סייבר, מסמך 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 "אבטחת העברה מנוהלת של קבצים (MFT)" מתמקד בהמלצות ליישום לשם אבטחת המערכת הטכנולוגית והארגון העושה בה שימוש.

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 מערכת העברה מנוהלת של קבצים (MFT)

פרק זה סוקר את האיומים העיקריים הנגזרים מתקיפת מערכת MFT:

	שם האיום	תיאור
.1	מניעת שירות - (DOS Denial of service)	תוקף עשוי לגרום לשיבוש פעילות מערכת ה-MFT, עד לכדי השבתתה. פעולה זו עשויה לפגוע בתהליכים עסקיים אשר תלויים בתקינות זרימת המידע.
.2	החדרת נוזקה	תוקף עשוי להשתמש בממשק העברת הקבצים לשם החדרת קובץ המכיל נוזקה לרשת הארגון.
.3	ציתות (Eavesdropping)	תוקף עשוי ליירט מידע העובר על גבי רשת ציבורית (דוגמת האינטרנט), ולאחר מכן לבצע פעולות שונות במטרה לפענחו.
.4	תקיפת האדם שבאמצע (MiTM)	תוקף עשוי לממש תקיפת האדם שבאמצע וזאת במטרה לשנות ניתוב של חבילות המידע או להזריק נוזקה/קוד זדוני לתעבורה לגיטימית.
.5	שנמוך פרוטוקול (Downgrade Attack)	תוקף עשוי לכפות אל המערכת לעשות שימוש בפרוטוקול בעל חולשות ידועות (דוגמת SSL 2.0), דבר אשר יאפשר לו לנצל חולשות אלו למטרותיו.

	שם האיום	תיאור
.6	הדלפת מידע (Data Leakage) מכוונת	תוקף עשוי לעשות שימוש במערכת לשם הדלפת מידע באופן ישיר או עקיף (דוגמת הוספת מידע נלווה לקובץ לגיטימי).
.7	השגת פרטי אימות	תוקף עשוי להשיג פרטי אימות של משתמש לגיטימי, ובהתאם לעשות שימוש לרעה בהם. בין השיטות להשגת פרטי אימות אלו ניתן למנות לדוגמא: א. תקיפת כוח (Brute Force Attack) או תקיפת מילון (Dictionary Attack) או תקיפת "יום הולדת" (Birthday Attack). ב. צפייה במשתמש מקליד סיסמה (Shoulder Surfing). ג. פישינג (Phishing). ד. SQLi לממשק ההזדהות. ועוד
.8	השתלטות על ממשקי ניהול (לרבות API אשר חשוף לאינטרנט)	תוקף עשוי להשתלט על ממשק הניהול, דבר אשר עשוי לאפשר: א. קבלת גישה למידע רגיש/חסוי המאוחסן או המשונע על-ידי המערכת. ב. שינוי ניתוב הקבצים, כך שהם יועברו ליעד הנמצא בשליטתו. ג. החדרת נוזקה לקובץ חדש או לקובץ לגיטימי.
.9	מידור לקוי עקב טעות אנוש בהחלת הגדרות תצורה	טעות אנוש בהגדרת תצורה (Misconfiguration) עשויה לגרור מידור לקוי בין משתמשים לגיטימיים במערכת, דבר אשר עשוי ליצור חשיפה שלא לצורך.
.10	הדלפת מידע (Data Leakage) עקב טעות אנוש	טעות אנוש בהגדרת תצורה עשויה לגרור שליחת קבצים לנמען השונה מזה הרצוי.

	שם האיום	תיאור
.11	התכחשות מקבל הקובץ (Repudiation)	הגורם המקבל עשוי להתכחש לקבלת הקובץ, דבר אשר עשוי לחשוף את הארגון לסנקציה משפטית או סנקציה אחרת.
.12	אי שלמות ומהימנות הקבצים (Integrity)	תקלה תפעולית או תקיפת סייבר עשויה לגרום לאי שלמות ומהימנות הקבצים.
.13	פגיעה בזמינות קבצים במקור	תקלה תפעולית או תקיפת סייבר עשויה לגרום לשינוי כיוון התעבורה ודריסה של קבצים במקור.
.14	טכנולוגיית מידע צללים (Shadow IT)	גורמים שונים בארגון עשויים לעשות שימוש בפתרון עצמאי בניגוד לנוהל העבודה הרשמי, ובכך ליצור חשיפה לא מבוקרת לארגון.

טבלה 5: איומים הנגזרים מתקיפת העברה מנוהלת של קבצים (MFT)

6. המלצות ליישום - אבטחת העברה מנוהלת של קבצים (MFT)

פרק זה מציג רשימה של המלצות ליישום, אשר מימוש נכון שלהן יסייע באבטחת מערכת MFT:

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
המלצות כלליות		
.1	מומלץ כי הארגון יוודא כי הגדיר במערכת ה-MFT מדיניות למחזור החיים של הקבצים (object retention, placement, protection, transition, and expiration)	
.2	מומלץ כי הארגון יוודא כי הגדיר במערכת ה-MFT שטח אחסון (Quota) ייעודי לכל משתמש.	
.3	מומלץ כי הארגון יוודא שהוגדרו במערכת ה-MFT ספים (Bars) ורפים (Thresholds). דוגמאות ליישום: א. הגדרה של מספר קבצים הניתנים להעלאה סימולטאנית ברמת-על- וברמת משתמש ספציפי ב. הגדרה של מספר קבצים הניתנים להורדה סימולטאנית ברמת-על- וברמת משתמש ספציפי	
הקשחה		
.4	מומלץ כי הארגון יוודא כי הרכיבים הוטמעו בהתאם לעקרון פונקציונאליות נמוכה (Least Functionality). דוגמא ליישום: ה-PEP ישמש למטרה ספציפית ומוגדרת בלבד.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.5	מומלץ כי חשבונות שירותי המערכת של ה-MFT יעשו שימוש בהרשאות נמוכות (Least Privilege).	
.6	מומלץ כי הארגון יוודא קיומה של הפרדה במחיצות/כוננים ה-PEP כדלקמן: א. מחיצה ייעודית למערכת ההפעלה. ב. מחיצה ייעודית לתוכנת ה-MFT. ג. מחיצה ייעודית לאחסון קבצי המשתמשים.	
.7	מומלץ כי הארגון יוודא כי מערכת הקבצים המחזיקה את ה"כספות" ותוכנת ה-MFT של שרת ה-PEP הקדמי, תהיה שונה משל ה-PEP האחורי. דוגמא ליישום: שרת ה-PEP הקדמי יעשה שימוש ב-XFS שרת ה-PEP האחורי יעשה שימוש ב-NTFS	
.8	מומלץ כי הארגון יוודא כי רכיבי מערכת ה-MFT הוקשחו בהתאם למתודולוגית הקשחה מקובלת. להרחבה ראו: המלצות ליישום - הקשחת מערכות מחשוב https://www.gov.il/he/departments/general/systemhardening	
.9	מומלץ כי הארגון יוודא כי רכיבי המערכת (לא כולל קבצי המשתמשים) יחזרו למצב אפס (Steady State) באופן עתי. ככלל, לכל הפחות יש להחזיר את ה-PEP למצב אפס אחת ל-12 שעות.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.10	מומלץ כי הארגון יוודא כי רכיבי המערכת חסינים בפני שידור מידע היסטורי (Replay Attack).	
.11	מומלץ כי הארגון יוודא כי לא ניתן לכפות על רכיבי מערכת ה-MFT לעשות שימוש בפרוטוקול ישן מזה אשר הוגדר (Downgrade Attack).	
.12	מומלץ כי הארגון יוודא שמערכת ה-MFT מבצעת מחיקה של הקבצים כך שלא ניתן לאחזרם. בכלל זה, מומלץ לוודא תאימות של המחיקה לתקנים מקובלים, דוגמת ISO/IEC 21964 (DIN 66399).	
.13	מומלץ כי ה-PEP יאפשר אחסון/שינוע של קבצים בהתאם לרשימה לבנה של פורמטים (True Type).	
.14	מומלץ כי הארגון יוודא כי לא ניתן להוסיף מידע לא מורשה לקבצים אשר מערכת ה-MFT מאחסנת, משנעת או מעבדת [קרי, דלף מידע באמצעות ערוץ סמוי (Covert Channel)].	
.15	מומלץ כי הארגון יוודא כי רכיבי מערכת ה-MFT פועלים בסביבה מבודדת, כך שפגיעה בהם לא תשפיע על רכיבים/יישומים אחרים ומערכת ההפעלה (Application Isolation).	
דרישות ארכיטקטורה		
.16	מומלץ כי הארגון יישם עקרונות מקובלים לקיטוע רשתי (Network Segmentation/Network Isolation) - חלוקת הרשת לאזורי ניהול קטנים, וזאת על סמך פונקציונאליות יעד ההגנה ורמת הסיכון. דוגמאות ליישום: א. כל רכיב (PAP, PDP, PEP Frontend, PEP Backend, PIP, PRP) יעשה שימוש ברשת ייעודית.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	ב. שימוש ב-Microsegmentation	
.17	מומלץ כי הארגון יישם עקרונות מקובלים למידור רשתי (Network Segregation) - אכיפת כללי גישה בין יעדי הגנה החולקים רשת משותפת. יש לתת את הדעת לסינון תעבורה בין המכונות הווירטואליות (East-West Traffic) אשר אינה עוברת דרך ה-FW הרשתי. דוגמאות ליישום: ג. שימוש ב-FW רשתי. ד. שימוש ב-Distributed FW	
.18	מומלץ כי הארגון יוודא כי שעון רכיבי המערכת מסונכרן מול שעון זמן מהימן, וזאת תוך מניעת אפשרות לניצול לרעה של ערוץ זה (דוגמת התחזות לשעון זמן מהימן).	
.19	מומלץ כי הארגון יוודא כי ניתן לאמת את מקוריות/אותנטיות (Authenticity) הקבצים אשר מערכת ה-MFT מאחסנת בהווה, ואחסנה בעבר. דוגמא ליישום: שימוש ב- פנקסים מבוזרים (DLT- Distributed Ledger Technology) או בפתרון אחר העומד בדרישות חוק חתימה אלקטרונית.	
.20	מומלץ כי הארגון יוודא כי לאחר כל העברת קובץ באמצעות מערכת ה-MFT, נשלחת הודעה לרכיב השולח כי הקובץ התקבל, כך שהגורם המקבל לא יוכל להתכחש לביצוע הפעולה (Non-Repudiation). דוגמא ליישום: שימוש בפרוטוקול AS4	
אבטחת העברת קבצים בין שרת המקור (דוגמת שרת הקבצים) ל-PEP האחורי		

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.21	מומלץ כי הארגון יוודא כי שרת המקור (דוגמת שרת הקבצים) מבצע דחיפה (Push) של הקבצים ל-PEP האחורי.	
.22	מומלץ כי הארגון יוודא שלפני הגעת הקבצים ל-PEP האחורי הוא יבצע הסרת מידע שאינו חיוני. דוגמא ליישום: שימוש במערכת השחרה (Cleansing System)	
.23	מומלץ כי הארגון יוודא לפני הגעת הקבצים ל-PEP האחורי כי אין דלף מידע לא רצוני. דוגמא ליישום: שימוש במערכת DLP	
.24	מומלץ כי הארגון יוודא כי קבלת קבצים מה-PEP האחורי תתבצע במשיכה (Pull) וביוזמת שרת המקור (דוגמת שרת הקבצים).	
אבטחת העברת קבצים בין PEP אחורי, ל-PEP קדמי		
.25	מומלץ כי הארגון יוודא כי ה-PEP האחורי מבצע דחיפה (Push) של הקבצים ל-PEP הקדמי.	
.26	מומלץ כי הארגון יוודא כי קבלת קבצים מה-PEP הקדמי תתבצע במשיכה (Pull) וביוזמת ה-PEP האחורי.	
.27	מומלץ כי הארגון יוודא כי לפני הגעת הקבצים ל PEP האחורי, הקבצים יזוכו מפני נוזקות (Malwares)[3]. דוגמאות ליישום: ה. שימוש במערכת הלבנה (Data-Sanitization) אשר ה-PEP הקדמי פונה אליה באמצעות פרוטוקול ICAP.	

[3] זיהוי קבצים - תהליך אשר בסופו ניתן להבטיח כי הקבצים אינם מכילים נוזקות

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	ו. שימוש במערכת הלבנה (Data-Sanitization) המשמשת כגורם מתווך בין ה-PEP הקדמי, ל-PEP האחורי.	
.28	מומלץ כי הארגון יוודא כי ה-PEP הקדמי, וה-PEP האחורי עושים שימוש באימות הדדי (Mutual Authentication). דוגמא ליישום: שימוש ב-mTL	
.29	מומלץ כי הארגון יוודא כי ה-PEP הקדמי אינו מכיל קבצים בשגרה, ורק לאחר השלמת הזדהות מוצלחת, הקבצים יועתקו ל-PEP הקדמי בהתאם לדרישת המשתמש, ולאחר זמן נתון יימחקו באופן ממוכן.	
אבטחת תהליך רישום משתמשים (Onboarding\Enrolment)		
.30	מומלץ כי הארגון יוודא כי שלב הרישום יתבצע שלא בצורה ישירה מול מערכת ה-MFT, אלא לאחר הרשמה מול "אזור אישי" או הזדהות חזקה מול מערכת הזדהות ייעודית אחרת.	
אבטחת תהליך הזדהות (Authentication) משתמשים		
.31	מומלץ כי הארגון יוודא כי ה-PEP הקדמי אינו מאפשר הזדהות של חשבונות משתמשים פנים ארגוניים.	
.32	מומלץ כי הארגון יוודא כי ה-PEP הפנימי אינו מאפשר הזדהות של חשבונות משתמשים מחוץ לארגון.	
.33	מומלץ כי הארגון יוודא כי הוא אוכף מדיניות סיסמאות בהתאם למדיניות המאושרת.	
.34	מומלץ כי הארגון יוודא כי הוא נועל חשבונות לאחר X ניסיונות גישה לא מורשים.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.35	מומלץ כי הארגון יוודא כי גישה של משתמש אנושי תחייב השלמה מוצלחת של אימות רב-גורמי (MFA). במקרה של מנהל מערכת יש לוודא אכיפה של גישה בהתאם לכתובת IP מקור.	
.36	מומלץ כי הארגון יוודא כי גישה של משתמש מכונה תחייב השלמה מוצלחת של אימות רב-גורמי (MFA), הכולל אימות הדדי (Mutual Authentication) והגבלה לפי כתובת IP מקור.	
.37	מומלץ כי הארגון יוודא כי הוא עושה שימוש בעקרונות מקובלים לאימות מסתגל (Adaptive Authentication). להרחבה ראו: חיזוק זיהוי משתמשים במערכות ותשתית של ארגונים ע"י שימוש באימות רב-גורמי https://www.gov.il/he/departments/general/mfa	
.38	מומלץ כי הארגון יוודא כי ה-PEP האחורי והקדמי אינם מאפשרים גישה של לקוח שאינו עושה שימוש ברכיבי תוכנה עדכניים (דוגמת גרסת דפדפן עדכנית).	
.39	מומלץ כי הארגון יוודא כי לאחר X דקות ללא פעילות המשתמש, ה-PEP יזם ניתוק (Session Timeout).	
.40	מומלץ כי הארגון יגביל את מספר הפעילויות (Sessions) המותרות בו-זמנית של משתמש בודד. ככלל, אין לאפשר יותר מפעילות יחידה בזמן נתון.	
אבטחת תהליך בקרת גישה / ניהול הרשאות (Authorization)		
.41	מומלץ כי הארגון יוודא כי הוא עושה שימוש בבקרת גישה מסוג ""גישה מבוססת סיכון מסתגל"" (RAdAC - Risk Adaptive-Based Access Control) , על פי גישה זו, מתבצעת הרחבה למודל גישה מבוסס תכונה	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	(ABAC), כך שהרשאות המשתמש נקבעות בזמן הריצה בהתאם לתכונות שונות ותוך התחשבות ברמת הסיכון. בסביבת ענן המימוש השכיח למודל זה הינו ". Risk-Based Conditional Access	
.42	מומלץ כי הארגון יוודא כי לשם גישה לכספת/קובץ ע"י גורם שאינו הלקוח הרשמי, נדרש אישור סימולטאני של שני גורמים בלתי-תלויים (Dual Control).	
.43	מומלץ כי הארגון יוודא כי מתן גישה למערכת ה-MFT יתבצע בהתאם לעקרון הצורך לדעת (Need to Know).	
דרישות קריפטוגרפיה		
.44	מומלץ כי הארגון יוודא כי בעת מנוחה ושינוע כל קובץ יוצפן ע"י מפתח הצפנה הייחודי לו. ככלל, ארגונים הנדרשים לרמת אבטחה גבוהה יעשו שימוש בשתי שכבות הצפנה בלתי תלויות , העושות שימוש בשני מפתחות הצפנה ייחודים.	
.45	מומלץ כי הארגון יוודא כי שינוע קובץ יעשה על גבי תווך מוצפן. דוגמא ליישום: שימוש ב-TLS v1.3	
.46	מומלץ כי הארגון יוודא כי תהליך חילול מפתחות ההצפנה הוא בעל אנטרופיה גבוהה, המונעת אפשרות לניחוש מפתח ההצפנה או השפעה על תהליך החילול שלו.	
.47	מומלץ כי הארגון יוודא כי במסגרת ביצוע תהליכים קריפטוגרפים לא נחשף מידע ערכי בערוץ-צד (Side Channel).	
.48	מומלץ כי הארגון יוודא כי מפתחות פרטיים ותעודות דיגיטליות ו"סודות" (Secrets) יאוחסנו בהתקן בעל מנגנונים מקובלים כנגד חבלה (Tampering Resistance) וחשיפת חבלה (Tamper Evident).	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	ככלל יש להעדיף לעשות שימוש בהתקני HSM העומדים בדרישות תקנים מקובלים, דוגמת Common Criteria EAL 4 or Higher	
.49	מומלץ כי הארגון יוודא כי האלגוריתמים הקריפטוגרפים עומדים בדרישות תקן FIPS 140-2 Level 3 ומעלה.	
.50	מומלץ כי הארגון יוודא כי אינטגרציה עם KMS חיצוני תעשה באמצעות שימוש בפרוטוקול KMIP מקובל.	
.51	מומלץ כי הארגון יוודא כי גם במקרה שתוקף השיג נגישות מלאה לקובץ/מסד הנתונים של הסיסמאות, הוא לא יוכל לאחזרן. דוגמא ליישום: שימוש ב-Pepper	
.52	מומלץ כי הארגון יוודא כי גם במקרה שתוקף השיג גישה לסיסמת המשתמש, הוא לא יוכל לאחזרה. דוגמא ליישום: שימוש ב-Hash + Salt	
.53	מומלץ כי הארגון יוודא כי מערכת ה-MFT מבצעת שימוש במנגנונים קריפטוגרפים על מנת להגן על שלמות רשומות וכלי הבקרה.	
.54	מומלץ כי הארגון יוודא כי בעת ניסיון לאחזור סיסמה, כוח העיבוד אשר יידרש להשקיע יעלה באופן ליניארי.	
.55	מומלץ כי הארגון יוודא כי האלגוריתמים הקריפטוגרפים במערכת ה-MFT מספקים חסינות בפני מחשוב קוואנטי.	
.56	מומלץ כי הארגון יוודא באופן עתי כי הקבצים במערכת ה-MFT אינם מכילים נוזקות, וזאת על-ידי שימוש במנגנון שאינו חושף את תוכן הקבצים למשתמשים/מנהלי המערכת.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	דוגמא ליישום: שימוש בעקרון Zero-knowledge proof	
.57	מומלץ כי הארגון יוודא כי ה-PEP מוודא את שלמות ומהימנות (Integrity) הקובץ ע"י שימוש באמצעים קריפטוגרפיים, וזאת בטרם אישור ביצוע הפעולה למשתמש.	
.58	מומלץ כי הארגון יוודא כי רכיבי מערכת ה-MFT ממשים עקרונות מקובלים בהנדסת תוכנה, דוגמת אַטוֹמִיוּת, עִקְבִיוּת, בִּידוּד וְעַמִידוּת - (ACID Atomicity, Consistency, Isolation, Durability).	
עדכוני אבטחה (פאצ'ים) וניהול גרסאות		
.59	מומלץ כי הארגון יוודא החלת עדכוני אבטחה תוך שלושה ימים מיום פרסומם. יש לתת את הדעת לנושא החלת עדכוני האבטחה לסוכן (Agent) בנכסי הסייבר.	
.60	מומלץ כי הארגון יוודא שדרוג לגרסה עדכנית תוך שלושה ימים מיום פרסומם. יש לתת את הדעת לנושא שדרוג סוכן (Agent) בנכסי הסייבר.	
ביקורות		
.61	מומלץ כי הארגון יוודא באופן עתי כי אין במערכת ה-MFT חשבונות משתמשים שאינם נדרשים לעבודה שוטפת. בכלל זה, יש לבצע הבחנה בין חשבונות משתמשים רגילים, לחשבונות משתמשים חזקים.	
.62	מומלץ כי הארגון יוודא באופן עתי את רמת ההרשאות אשר הוקצתה לכל משתמש במערכת ה-MFT.	
.63	מומלץ כי הארגון יוודא באופן עתי כי מערכת ה-MFT אינה מאחסנת, מעבדת או משנעת קבצים ברמת סמך גבוהה מזו שהוגדרה במקור.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.64	מומלץ כי הארגון יוודא באופן עתי כי מערכת ה-MFT אינה מאחסנת קבצים שאינם נדרשים לעבודה שוטפת.	
.65	מומלץ כי הארגון יוודא באופן עתי כי מערכת ה-MFT אינה מאפשרת/משמשת לטובת דלף מידע.	
.66	מומלץ כי הארגון יבצע בדיקות חוסן עיתיות למערכת ה-MFT.	
שרשרת אספקה		
.67	מומלץ כי הארגון יוודא כי ספקי השירות הרלוונטיים עומדים בדרישות מתודת שרשרת האספקה[4] של המערך.	
תיעוד וניטור		
.68	מומלץ כי הארגון יוודא כי מערכת ה-MFT מבצעת תיעוד ביומן רישום אוטומטי וייעודי (רישום Log) כל יצירה, שינוי, אפשור, ניטרול והסרה של חשבון משתמש.	
.69	מומלץ כי הארגון יוודא כי מערכת ה-MFT מבצעת תיעוד ביומן רישום אוטומטי וייעודי (רישום Log) מתן הרשאה, שינוי, אפשור, והסרה הרשאה.	
.70	מומלץ כי הארגון יוודא כי מערכת ה-MFT מבצעת תיעוד ביומן רישום אוטומטי וייעודי (רישום Log) של פעולות יצירה, קריאה, עדכון ומחיקה (CRUD - Create, Read, Update, and Delete).	
.71	מומלץ כי הארגון יוודא כי מערכת ה-MFT כוללת מנגנון לשליחת התראה במידה של הפסקת כתיבת נתונים ללוגים/ייצור לוגים.	

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

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.72	מומלץ כי הארגון יוודא כי מערכת ה-MFT כוללת מנגנון המאפשר ניטור פעילות חשבונות לזיהוי שימוש חריג, וידווח על שימוש חריג לבעלי התפקידים המתאימים.	
.73	מומלץ כי הארגון יוודא כי מערכת ה-MFT תקושר למערכת הניטור הארגונית (SIEM).	

טבלה 6: המלצות ליישום לשם אבטחת מערכת MFT

ארגונים אשר מעוניינים לשפר את רמת האבטחה יכולים לבצע אינטגרציה עם פתרון DRM (Digital Rights Management), אשר מאפשר שליטה ובקרה משופרת על השימוש בקבצים בארגון ומחוצה לו.

7. נספחים (Appendixes)

פרק זה מכיל את רשימת הנספחים הנלווים למסמך זה.

נספח 1 – אבטחת העברה מנוהלת של קבצים (MFT)

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.

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
ACID	Atomicity, Consistency, Isolation, Durability
ACL	Access Control List
ADC	Application Delivery Controllers
API	Application Programming Interface
B2B	Business to Business
BCP	Business Continuity Planning
CRUD	Create, Read, Update, and Delete
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
DNS	Domain Name System
DoS	Denial of Service
DR	Disaster Recovery
DRM	Digital Rights Management
EAL	Evaluation Assurance Level
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
FTPS	FTP Secure / FTP-SSL
GSLB	Global Server Load Balancing
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
ICAP	Internet Content Adaptation Protocol
IEEE	Institute of Electrical and Electronics Engineers
IOC	Indicator of Compromise
IOE	Indicator of Exposure

שם המונח	ביאור
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
KMIP	Management Interoperability Protocol
KMS	Key Management Server
MFT	Managed File Transfer
MiTM	Man-in-the-Middle Attack
NTFS	New Technology File System
OSI	Open Systems Interconnection
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PEP	Policy Enforcement Point
PRP	Policy Retrieval Point
QoS	Quality of Services
RAdAC	Risk Adaptive-Based Access Control
RAM	Random-Access Memory
REST	Representational State Transfer
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAS	Shared Access Signature
SDK	Software Development Kit
SFTP	SSH FTP
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SQLi	SQL Injection
SSH	Secure Shell
SSL	Transport Layer Security
TLS	Secure Sockets Layer
TTL	Time to Live
URI	Uniform Resource Identifier

שם המונח	ביאור
URL	Uniform Resource Locator
WAF	Web Application Firewall
XACML	eXtensible Access Control Markup Language

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

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

היערכות כנגד תקיפות מניעת שירות מבוזרות (DDoS) - המלצות ליישום

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

מדיניות לאומית להזדהות בטוחה

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

חקיקה

תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017

חוק חתימה אלקטרונית תשס"א-2001

חוק הגנת הפרטיות, תשמ"א-1981

חוק הארכיונים, תשט"ו-1955

כללי

מקורות מידע באנגלית:

General

AAA Authorization Framework, RFC 2904

- ✓ https://tools.ietf.org/html/rfc2904

Control-M

- ✓ https://www.bmc.com/it-solutions/control-m-managed-file-transfer.html

Accellion

- ✓ https://www.accellion.com/platform/simple/managed-file-transfer/

Go Anywhere

- ✓ https://www.goanywhere.com/solutions/managed-file-transfer

OWASP API Security

- ✓ https://owasp.org/www-project-api-security/

Password Storage Cheat Sheet

- ✓ https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

NIST

SP 1800-11a: Executive Summary

- ✓ https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/recover

***** סוף מסמך *****