סייבר ישראל
מערך הסייבר הלאומי

המלצות ליישום (Best Practices) שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור

סייבר ישראל
מערך הסייבר הלאומי

המלצות ליישום
(Best Practices)

שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור

פברואר
2021

תוכן עניינים

>>>> שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור

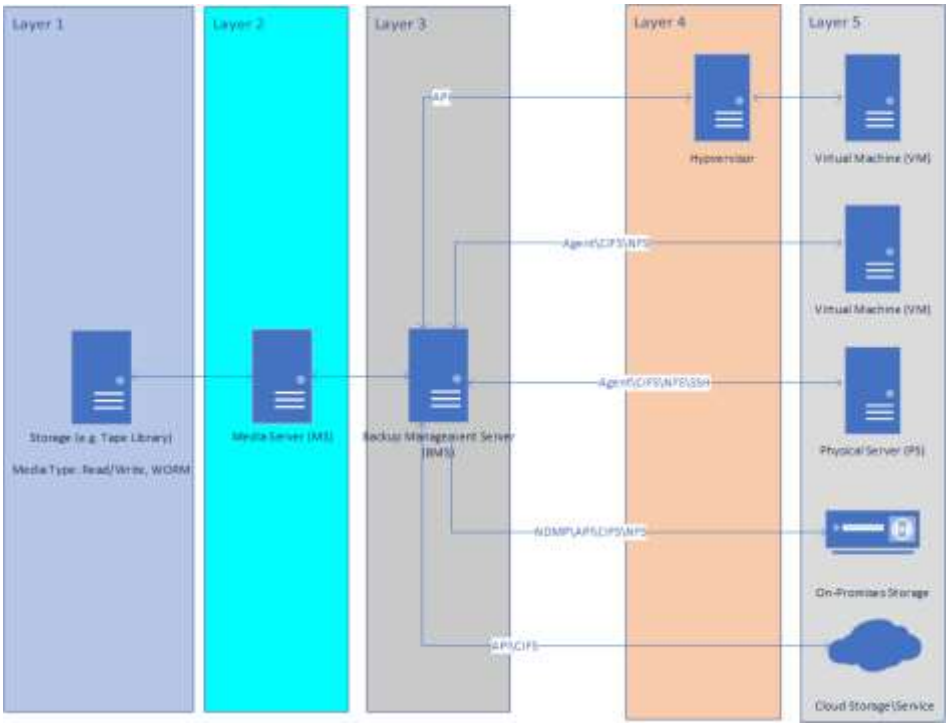
1. מבוא (Introduction)

1.1 כללי

בשנים האחרונות החלה עלייה בתדירות ואיכות תקיפות סייבר אשר מטרתן לפגוע בזמינות ו/או מהימנות המידע המאוחסן בארגון. בכלל זה, ניתן לראות תקיפות כופרה (Ransomware) אשר מונעות גישה למידע ע"י הצפנת תוכנו, וזאת בשילוב שיטות שונות אשר מטרתן לפגוע ביכולת הארגון לשחזר מידע אשר נשמר כתמונת מצב (Snapshot) בסביבה הוירטואלית או הפיזית ובמערך גיבוי הנתונים. כמו כן, ניתן לראות כי תוקפים שונים במרחב הסייבר עושים שימוש בנוזקות המשמידות מידע (Wiper), דבר הכולל מחיקה של קושחה (Firmware) ופגיעה מכוונת במערך הגיבוי.
ארגונים אשר עושים שימוש בשיטות גיבוי מסורתיות, דוגמת אחסון מידע בקלטות, נחשפים לאתגרים דוגמת גיבוי נפחי מידע הגדלים מיום ליום והצורך לגבות מידע באתרים מרוחקים ושירותי ענן, וזאת לצד דרישות עסקיות לביצוע תהליכי התאוששות בזמן קצר.
לאור זאת עולה חשיבות לשילוב עקרונות הגנת הסייבר בתהליכי הגיבוי והשחזור.

1.2 ארכיטקטורה טיפוסית של מערך גיבוי נתונים

להלן תרשים של ארכיטקטורה טיפוסית של מערך גיבוי נתונים:



תרשים 1: ארכיטקטורה טיפוסית של מערך גיבוי נתונים

להלן סקירה של תפקיד של כל שכבה:

מס'	שם השכבה	תפקיד
.1	אחסון מידע/מדיית אחסון (Storage)	שכבה זו אחראית לאחסון המידע המגובה.
.2	שרת ניהול המדיה (MS - Media Server)	שכבה זו אחראית לניהול מדיות הגיבוי.
.3	שרת ניהול הגיבוי (BMS - Backup Management Server)	שכבה זו אחראית לניהול משימות הגיבוי/השחזור מול לקוחות מערך הגיבוי.

.4	שרת מארח שרת ניהול סביבה וירטואלית (Hypervisor)[1]	שכבה זו אופציונאלית, ומהווה גורם מתווך בין שרת ניהול הגיבוי לקוחות/נכסי סייבר מסוג מכונות וירטואליות.
.5	לקוחות מערך הגיבוי	שכבה זו מכילה את הלקוחות אשר מחזיקים את המידע אשר בשגרה נדרש לגבותו.

טבלה 1: תפקיד שכבות מערך גיבוי נתונים

ראוי לציין כי שרת ניהול הגיבויים עשוי לעשות שימוש בשיטות עבודה שונות לשם התקשרות עם הלקוחות.
להלן סקירה של מספר שיטות שכיחות:

מס'	שם השיטה	תיאור
.1	שימוש בסוכן (Agent)	בשיטת עבודה זו הארגון נדרש להתקין תוכנת סוכן מטעם יצרן תוכנת הגיבוי על לקוח מערך הגיבוי (דוגמת שרת מסד נתונים), ושרת ניהול הגיבוי המנהל את משימות הגיבוי/שחזור ישירות. במקרים אלו מותקנת שכבת אינטגרציה מול האפליקציה.
.2	שימוש בממשק תכנות יישומים (API)	בשיטת עבודה זו הארגון עושה שימוש ב-API אשר יצרן הלקוח החצין עבורו, ושרת ניהול הגיבוי המנהל את משימות הגיבוי/שחזור מולו.
.3	שימוש בפרוטוקול NDMP (Network Data Management Protocol)	בשיטת עבודה זו הארגון עושה שימוש בפרוטוקול NDMP בעת עבודה עם לקוח מסוג NAS (Network Attached Storage), ושרת ניהול הגיבוי המנהל את משימות הגיבוי/שחזור ישירות. שיטת עבודה זו נחשבת בדרך כלל כיעילה בעת גיבוי NAS, אך היא עשויה לעיתים לסבול ממגבלות שונות, דוגמת העדר

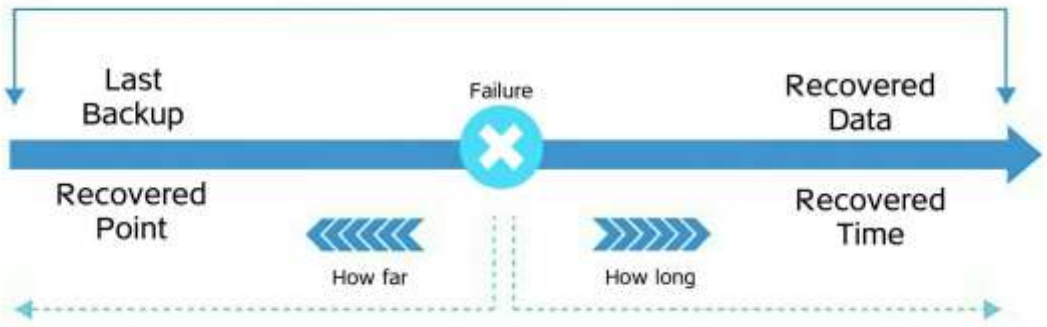
[1] שם חלופי: מערכת הפעלה עילית

		יכולת שחזור של המידע על NAS תוצרת יצרן אחר או קושי לשחזר באופן אפקטיבי "מידע חי".
.4	שימוש בשרת מארח (Hypervisor)/שרת ניהול סביבה וירטואלית	שיטה זו מהווה הרחבה לשיטת העבודה ב-API, וזאת כאשר השרת המארח (או השרת המנהל את הסביבה הווירטואלית) משמש כגורם מתווך (פרוקסי) בין שרת ניהול הגיבוי למכונות הווירטואליות.
.5	העתקת קבצים באמצעות פרוטוקול שיתוף קבצים ללא שימוש בכלי צד שלישי	בשיטת עבודה זו הארגון עושה שימוש בפרוטוקול מקובל (דוגמת NFS\CIFS) לשיתוף קבצים, ללא שימוש בכלי צד שלישי. למרות זמינותה הגבוהה של שיטה זו, היא נחשבת לפחות מתאימה לגיבוי נפחים גדולים או למספר לקוחות סימולטנית, ואף אינה מתאימה למצבים בהם נדרש לגבות "מידע חי".
.6	העתקת קבצים באמצעות פרוטוקול שיתוף קבצים וזאת תוך שילוב יכולות מתקדמות של תוכנת הגיבוי	בשיטת עבודה זו הארגון עושה שימוש בפרוטוקול מקובל (דוגמת NFS\CIFS) לשיתוף קבצים, תוך שילוב יכולות מתקדמות של תוכנת הגיבוי או יצרן החומרה. בין היכולות המתקדמות ראוי לציין את קיומו של מנגנון המאפשר גילוי וזיהוי מהיר של קבצים שהשתנו יחסית לזמן הגיבוי הקודם שלהם (Change File Tracking) או שמתממשקות למנגנון זהה המסופק ע"י יצרן חומרה התומך באפשרות זאת. לאור זאת, שיטה זו מתאימה לגיבוי נפחים גדולים או למספר לקוחות סימולטנית, ואף מתאימה למצבים בהם נדרש לגבות "מידע חי".
.7	העתקת קבצים באמצעות פרוטוקול ניהול	בשיטת עבודה זו הארגון עושה שימוש בפרוטוקול ניהול מקובל (דוגמת SSH) להעתקת קבצים. שיטה זו מתאימה בעיקר לגיבוי הגדרות תצורה וקושחה של ציוד תקשורת ואמצעי הגנת סייבר.

טבלה 2: סקירת שיטות עבודה ליצירת קשר בין שרת ניהול הגיבוי ללקוחות

1.3 הקשר בין גיבויים לתוכנית המשכיות עסקית (BCP)

קיומה של תוכנית המשכיות עסקית אפקטיבית הינה נדבך חשוב בהצלחת הארגון לשמר רציפות תפקודית במקרה של אירוע סייבר, תקלה תפעולית, מלחמה או אירוע חריג אחר.
מקובל כי תוכנית המשכיות עסקית כוללת לכל תהליך עסקי / נכס סייבר מדדים מקובלים דוגמת נקודת השחזור הרצויה למידע (RPO - Recovery Point Objective) וזמן היעד להתאוששות (RTO - Recovery Time Objective), אשר אמורים לסייע לארגון בטיוב מיטבי של הדרישות ממערך הגיבוי.
ראוי לציין כי את ערך המדדים הנהלת הארגון צריכה לקבוע ולאשר זאת על סמך דרישות חוק, רגולציה (דוגמת יעדי השירות), דרישות חוזיות וצרכים עסקיים.
התרשים הבא סוקר את היחס בין ה-RPO\RTO לזמן הנדרש לשחזור מידע לנקודת זמן מסוימת:



תרשים 2: היחס בין ה-RPO\RTO לזמן הנדרש לשחזור מידע לנקודת זמן מסוימת

כך לדוגמה, בהינתן ה-RPO של נכסי סייבר פלוני (מערכת מחשוב) הינו שעה אחת, וכי ה-RTO הינו ארבע שעות, על הארגון לוודא כי:

א. ברשות הארגון גיבוי עדכני ותקין נכון לעד שעה לאחור.

ב. מדיית הגיבוי זמינה.

ג. מערך הגיבוי זמין לביצוע פעולות השחזור.

ד. גורמים טכנולוגיים ואחרים זמינים (לרבות זמינות בתנאי קיצון, דוגמת אפידמיה, שעות הלילה, שבתות וחגים).

ה. קיומה של כשירות נאותה מצד הגורמים המקצועיים.

ו. הזמן הנדרש להשלמת השחזור (MTTR - Mean Time to Recovery) הינו פחות מה-RTO, וזאת על-מנת להשאיר חלון זמן מספק להשלמת תהליכים תפעוליים משלימים עד לחזרה לשגרה.

ז. נכס הסייבר אליו המידע ישוחזר תקין ונקי מנוזקות (Malwares).

ראוי לציין כי במקרה של צורך לבצע שחזור של מספר נכסי סייבר במקביל ו/או במקרה של תפוקת מערך הגיבוי נמוכה מהרצוי, עולה חשיבות לסדר השחזור וזמינות כוח-אדם למשאבים אחרים, וזאת במטרה להבטיח חזרה לשגרה של תהליכי ליבה בשלב הראשוני, ורק בשלב המשני חזרה לשגרה של תהליכים שאינם קריטיים.
יוער כי במקרים מסוימים ארגונים עשויים להשיג ערך מקיום חוזה התקשרות מול ספק מומחה אשר יוכל לסייע בעת הצורך, כך שהארגון יוכל לבצע את השחזור בהתאם למדדים אשר הוגדרו.
כמו כן, על תוכנית המשכיות עסקית לכלול התייחסות למצבי קיצון, דוגמת הצורך לבצע שחזור מאפס באתר חלופי, תקלה במערך הגיבוי, תקלה או חבלה מכוונת במדיית הגיבוי ורשלנות בתפעול וכן הצורך לעמוד במדדי קיצון דוגמת RTO=0 ו-RPO=0.

ישנה חשיבות גבוהה לאשר באופן עתי את מדדי הגיבוי מול ההנהלה (וזאת מעבר לאישור תוכנית ה-BCP), תוך הבהרת משמעויות עסקיות נגזרות דוגמת מחלקות בחברה שיגובו ואלה שלא, כמויות מידע, סוגי מידע, עלויות וכד'.

קיומה של תוכנית המשכיות עסקית אפקטיבית מהווה אבן ליבה בפעולות הגנת הסייבר של הארגון. לאור העובדה כי לא ניתן להבטיח ב-100% מתן מענה אפקטיבי וקבוע כנגד תרחישי תקיפה ידועים ולא ידועים, יכולת הארגון לבצע התאוששות מאפס (לרבות השלמת דילוג לעבודה באתר חלופי) הינה קריטית.

2. מטרות ויעדים (Goals & Objectives)

מסמך זה מציג המלצות ליישום לשילוב עקרונות הגנת סייבר בתהליכי גיבוי ושחזור.

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 "**שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור**" מתמקד בהמלצות ליישום לשם הבטחה כי הארגון יוכל לבצע פעולות שחזור אפקטיביות במקרה הצורך.
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 מערך הגיבוי

פרק זה סוקר את האיומים העיקריים על מערך גיבוי נתונים:

	שם האיום	תיאור
1.	מניעת שירות (DOS - Denial of service)	א. תוקף עשוי לגרום לעומס חריג על מערך הגיבוי, כך שמשימות גיבוי לא יסתיימו במועד או לא יתבצעו כלל.

	שם האיום	תיאור
		ב. תוקף יכול לחדור לשרת הניהול ולגרום לתזמון מספר רב של משימות גיבוי. יצוין כי מעבר לפגיעה אפשרית ברמת השירות של שרת הניהול, הדבר עשוי לפגוע ברמת השירות של נכסי סייבר אחרים.
2.	רשלנות/טעות אנוש של גורם פנימי (דוגמת מנהל המערכת)[2]	א. עקב טעות אנוש/רשלנות מידע המאוחסן במדיית גיבוי עשוי להימחק או לעבור שינוי, כך שלא ניתן יהיה לעשות בו שימוש לשחזור נכס הסייבר. ב. עקב טעות אנוש/רשלנות מדיניות הגיבוי עשויה שלא להיאכף על נכס סייבר קיים או חדש, ולפיכך לא יהיה ניתן לבצע שחזור של המידע בעת הצורך. ג. טעות אנוש/רשלנות עשויה לגרום לשימוש בשיטת גיבוי לא מתאימה למאפייני נכס הסייבר [דוגמת מסד נתונים, שרת ניהול ספריה ארגונית (Directory Services) או שרת קבצים], אשר תמנע אפשרות לשחזור המידע באופן תקין. ד. שימוש במדיית אחסון מעבר למחזור החיים המומלץ (דוגמת MTBF) מעלה את הסבירות לקיומה של תקלה טכנית אשר תמנע אפשרות לשחזור תקין של המידע. ה. מדיית האחסון עשויה להינזק כתוצאה מתנאי סביבה לא נאותים (דוגמת טמפרטורה, לחות, שדה אלקטרומגנטי וחום).
3.	ניצול לרעה של הרשאות לגיטימיות	א. מנהל מערכת עשוי לעשות שימוש בהרשאות לגיטימיות לשם מחיקה/שינוי לא רצוני של מידע

[2] התמודדות ארגונית במרחב הסייבר עם האיום הפנימי
https://www.gov.il/he/departments/general/coping_thret

	שם האיום	תיאור
	(דוגמת מנהל המערכת)	המאוחסן במדיית הגיבוי. כך לדוגמה, ניתן להחיל משימת גיבוי חדשה לשם דריסת מידע קיים. ב. גורם אחר אשר השיג נגישות למחשב מנהל המערכת או לפרטי האימות של חשבונות מערך הגיבוי (דוגמת חשבון מערכת הגיבוי או ה- Agent Credentials), עשוי להשתמש בהרשאות לגיטימיות לשם מחיקה/שינוי לא רצוני של מידע המאוחסן במדיית הגיבוי.
4.	פעילות נוזקה	א. נוזקה עשויה לבצע פעולות זדוניות לשם מחיקה/שינוי לא רצוני של מידע המאוחסן במדיית הגיבוי. ב. מידע אשר הוצפן בטרם גיבוי ע"י כופרה, עשוי להיות משוחזר לסביבת הייצור, ובדיעבד יתגלה כי לא ניתן לעשות בו שימוש לטובת שחזור המידע. ג. מידע אשר הוצפן בטרם גיבוי ע"י כופרה, עשוי להיות משוחזר לסביבת הייצור, דבר העשוי להדביק את סביבת הייצור.
5.	דלף מידע עקב טעות אנוש/רשלנות (Data Leakage)	א. טעות אנוש/רשלנות עשויה לגרום לאחסון של המידע במקום הנגיש ללא מורשים. ראוי לציין כי סוגיה זו שכיחה בעת עבודה עם ענן ציבורי. ב. טעות אנוש/רשלנות עשויה לגרום לאובדן מדיית אחסון והגעתה לידי לא מורשים. ג. חשיפת מידע אודות מערך הגיבוי ו/או שיטות העבודה עשויה לסייע לתוקף פוטנציאלי בתכנון תקיפה ממוקדת כנגד הארגון.

	שם האיום	תיאור
.6	דלף מידע עקב זדון (Data Leakage)	א. גניבת מדיית אחסון. ב. שינוי זדוני של הרשאות ברירת מחדל עשוי לאפשר נגישות של המידע לידי לא מורשים. ג. משתמש בעל הרשאות לגיטימיות עשוי לעיין במידע אשר אינו מורשה לראותו. ד. חשיפת מידע אודות מערך הגיבוי ו/או שיטות העבודה עשויה לסייע לתוקף פוטנציאלי בתכנון תקיפה ממוקדת כנגד הארגון.
.7	פגיעה בזמינות קבצים במקור	תקלה תפעולית או תקיפת סייבר עשויות לגרום לשינוי כיוון התעבורה ודריסה של קבצים במקור.
.8	ציתות (Eavesdropping)	תוקף עשוי ליירט מידע העובר על גבי רשת ציבורית (דוגמת האינטרנט), ולאחר מכן לבצע פעולות שונות במטרה לפענחו.
.9	תקיפת האדם שבאמצע (MiTM)	תוקף עשוי לממש תקיפת האדם שבאמצע וזאת במטרה לשנות ניתוב של חבילות המידע או להזריק נוזקה/קוד זדוני לתעבורה לגיטימית.
.10	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 מערך הגיבוי. ב. שינוי ניתוב הקבצים, כך שהם יועברו ליעד הנמצא בשליטתו. ג. החדרת נוזקה לקובץ חדש או לקובץ לגיטימי.
.11	מחיקה או שינוי לא רצוני של	מחיקה או שינוי לא רצוני של אינדקס (קטלוג) הגיבוי בשרת ניהול הגיבוי עשויה לגרום לכך שלא ניתן יהיה לדעת היכן ממוקמים הגיבויים על

	שם האיום	תיאור
	אינדקס (קטלוג) הגיבוי	הדיסקים. יצוין כי במקרה שנעשה שימוש בקלטות ניתן לבצע בד"כ לבצע קריאה חוזרת מהקלטות דבר המשמר נגישות למידע, אך יוצר שיהוי ניכר בהשלמת תהליך השחזור.

טבלה 3: איומים עיקריים על מערך גיבוי נתונים

6. המלצות ליישום - שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור

פרק זה מציג רשימה של המלצות ליישום, אשר מימוש נכון שלהן יסייע בשילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור:

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
המלצות כלליות		
1.	מומלץ כי הארגון יוודא את קיומו של תהליך ארגוני להוספה/הסרה של נכסי סייבר למדיניות הגיבוי.	
2.	מומלץ כי הארגון יוודא כי ברשותו תוכנית המשכיות עסקית מעודכנת, לרבות קיומם של מדדים מקובלים (דוגמת RTO\RPO) לכל תהליך עסקי/נכס סייבר.	
3.	מומלץ כי הארגון יוודא את קיומו של תהליך ארגוני לגילוי וזיהוי מידע אשר נדרש לגבות, וזאת תוך התייחסות לנושאים מקובלים דוגמת הרשאות קיימות, מיקום פיזי ולוגי.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
4.	מומלץ כי הארגון יוודא כי הוא מכיר את ההשלכות הנגזרות על תהליכי הגיבוי והשחזור הנובעים משימוש בטכנולוגיות הקיימות בארגון. דוגמאות ליישום: א. שרתי מסדי נתונים שונים עושים שימוש במסגרת הפעילות בלוגים לשם תיעוד השינויים. ביצוע שחזור של מסד נתונים לגרסה של יום קודם עשוי לחייב "גלגול" של לוגים קיימים, וזאת עד להגעה לנקודת זמן הקרובה לרגע הכשל. ב. שרתי מסדי נתונים שונים עושים שימוש במסגרת הפעילות בלוגים לשם תיעוד השינויים. כשל בלוגים הקיימים בדיסק הקשיח של השרת עשוי למנוע אפשרות לשחזור המידע לנקודת זמן הקרובה לרגע הכשל.	
5.	א. מומלץ כי הארגון יוודא כי ברשותו מיפוי עדכני של דרישות חוק, רגולציה, דרישות חוזיות וצרכים אשר הוא כפוף להם בנושא משילות מידע (Data Governance) . בכלל זה, יש לוודא התייחסות לנושאים מקובלים דוגמת: ב. מגבלות אפשריות האוסרות אחסון מידע באתרים פיזיים/לוגים מסוימים. ג. אורך החיים לשמירה על המידע (Data Retention). ד. אורך החיים למחיקת מידע (Data Purging).	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	ה. דרישות רגולציה להמשכיות עסקית בהתאם למגזר הפעילות. ו. קיומן של דרישות אבטחה פרטניות. להלן דוגמא לחקיקה ורגולציה: ז. חוק הארכיונים, תשט"ו-1955 ח. חוק הגנת הפרטיות, תשמ"א-1981 ט. חוק חתימה אלקטרונית תשס"א-2001 י. תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017. יש לתת את הדעת לסוג מאגר המידע והדרישות הנגזרות מכך. יא. תקנות בריאות העם (שמירת רשומות), תשל"ז-1976. יש לתת את הדעת לסוג הרשומה הרפואית ומיקומה (ספק שירות/גוף בריאות וכד'). יב. פקודת מס הכנסה [נוסח חדש] יג. General Data Protection Regulation (GDPR)	
6.	מומלץ כי הארגון יוודא כי בחן באופן עתי את קיבולת מערך הגיבוי והתאמתו לצרכיו.	
7.	מומלץ כי הארגון יוודא שהגדיר במערך הגיבוי ספים (Bars) ורפים (Thresholds). דוגמאות ליישום: א. הגדרה של מספר גיבויים/שחזורים אשר ניתן להריץ בזמן נתון.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	ב. הגדרת תפוקה (Throughout) לתהליכי גיבוי/שחזור, וזאת ביחס לכל נכס סייבר. ג. חלון זמן לגיבוי/שחזור כל נכס סייבר.	
הקשחה		
8.	מומלץ כי הארגון יוודא כי חשבונות מערך הגיבוי יעשו שימוש בהרשאות נמוכות (Least Privilege). בכלל זה, יש לתת את הדעת לחשבונות בהם שרת ניהול הגיבוי עושה שימוש לשם גישה לנכסי הסייבר. דוגמאות ליישום: א. לשם גיבוי שרת מסד נתונים יוגדר חשבון ייעודי בעל הרשאות Read למסדי הנתונים הרלוונטיים. ב. לשם גיבוי שרת קבצים יוגדר חשבון ייעודי בעל הרשאות Read לקבצים הרלוונטיים. ג. חשבון מנהל המערכת אשר יעשה בו שימוש בשגרה לא יכיל יכולת לשנות מדיניות גיבוי קיימת.	
9.	מומלץ כי הארגון יוודא כי שרתי מערך הגיבוי לא ישרתו פונקציונאליות נוספת (Least Functionality).	
10.	מומלץ כי הארגון יוודא כי רכיבי מערך הגיבוי הוקשחו בהתאם למתודולוגית הקשחה מקובלת. להרחבה ראו: המלצות ליישום - הקשחת מערכות מחשוב https://www.gov.il/he/departments/general/systemhardening	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
הגנה על מדיות אחסון		
.11	מומלץ כי הארגון יוודא כי מדיות האחסון מאוחסנות במתקן חסין אש, אשר במקרה של הפעלת מערכת הכיבוי המידע לא יפגע. בכלל זה, יש לקבל המלצות מתאימות מיועץ כיבוי אש.	
.12	מומלץ כי הארגון יוודא כי לא ניתן לבצע שינוי/מחיקה למידע המאוחסן במדיות הגיבוי וזאת בתקופה אשר הוגדרה לשמירה על אורך חיי המידע (Data Retention). יש לתת את הדעת לשלוש תצורות עבודה מקובלות: א. החלת הגבלה רכה (Soft) - לאחר אכיפה של אורך החיים המינימלי לשמירת המידע, מנהל המערכת יכול לשנות את חלון הזמן שהוגדר. ב. החלת הגבלה קשיחה (Hard) - לאחר אכיפה של אורך החיים המינימלי לשמירת המידע, מנהל המערכת אינו יכול לשנות את חלון הזמן שהוגדר. חשוב לטובת התמודדות עם כופרה ו-Wiper. ג. החלת הגבלה קבועה (Permanent) - לאחר כתיבה לא ניתן לשנות/למחוק את המידע. חשוב לטובת התמודדות עם כופרה ו-Wiper.	
.13	מומלץ כי מערך הגיבוי יעשה שימוש ביכולות מקובלות למניעת חבלה (Tamper Resistant) ואיתור חבלה (Tamper-Evident). בכלל זה, יש לוודא כי לא ניתן לעקוף את המדיניות האוכפת אורך חיים מינימלי למידע ע"י שינוי לא רצוני של ערך השעון/תאריך המערכת.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.14	מומלץ כי הארגון יוודא כי המידע במדיות האחסון יוצפן באמצעות אלגוריתם סטנדרטי ועדכני. יש לתת את הדגש לשימוש בהצפנה במקרה שהמידע יאוחסן מחוץ לחצרות הארגון ו/או ישונע ברכב.	
.15	מומלץ כי הארגון יוודא כי אין תלות בין נקודות גיבוי, כך שניתן לבצע שחזור באופן מלא גם במקרה של כשל או תקלה בנקודת גיבוי קודמת.	
.16	מומלץ כי הארגון יוודא כי השימוש ביכולות מניעת כפילות (De-duplication) ודחיסה (Compression) אינן פוגעות באפקטיביות תהליך הגיבוי/השחזור.	
.17	מומלץ כי הארגון יוודא כי גם במקרה של העדר אינדקס של הגיבויים ניתן לבצע את פעולות השחזור, וזאת ללא פגיעה ברמות השירות המצופות.	
.18	מומלץ כי הארגון יוודא סימון לוגי/פיסי ברור ובולט של מדיות האחסון, וזאת תוך התייחסות לפרמטרים מקובלים, דוגמת: א. משך הזמן שיש למנוע שכתוב/שינוי של מידע במדיית האחסון ב. סיווג המידע ג. מקור המידע	
.19	מומלץ כי הארגון יוודא הקצאת מדיות אחסון ייעודיות למאגרי מידע רגישים (דוגמת מאגר ביומטרי או מאגר	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	כרטיסי אשראי), כך שלא יתבצע עירוב בין סוג מאגרי מידע שונים על אותה מדיית אחסון.	
20.	מומלץ כי הארגון יוודא כי מדיית האחסון נשמרת בהתאם להמלצות היצרן/בתנאים המאפשרים שמירה על תקינותה במשך תקופת זמן מוגדרת. דוגמא ליישום: אחסון קלטות גיבוי בכספת החסינה לאש ומים.	
גריטת מידע ומדיות אחסון		
21.	מומלץ כי הארגון ייבחן באופן עתי את הצורך לאחסון מידע במערך הגיבוי. בכלל זה, מומלץ לבחון ביצוע פעולות פרואקטיביות לצמצום איכותי/כמותי של המידע הקיים במערך הגיבוי (Data Minimization), וזאת במטרה א) להקטין את הנזק הפוטנציאלי במקרה של התרחשות אירוע סייבר, ב) להקטין את המוטיבציה לתקיפה של מערך הגיבוי. יש לתת את הדעת כי המידע במערך הגיבוי עשוי להוות "מאגר מידע" בהתאם להגדרת החוק או הרגולציה.	
22.	מומלץ כי הארגון יוודא מחיקה של מידע במדיות האחסון בהתאם לזמן הגריטה (Data Purging).	
23.	מומלץ כי הארגון יוודא שמערך הגיבוי מבצע מחיקה של הקבצים כך שלא ניתן לאחזרם. בכלל זה, מומלץ לוודא תאימות של המחיקה לתקנים מקובלים, דוגמת ISO/IEC 21964 (DIN 66399) או DoD 5220.22-M.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	במקרה של ענן ציבורי יש לבצע הצפנה של המידע מחוץ לספק הענן, ולאחר מכן למחוק את המפתח ולבצע מחיקה באמצעות האמצעים המומלצים ע"י ספק הענן (Crypto Shredding).	
.24	מומלץ כי הארגון יוודא שמצעי אחסון מידע של מערך הגיבוי יעברו בסוף מחזור החיים תהליך גריטה בהתאם לתקנים מקובלים ורגישות המידע, דוגמת ISO/IEC 21964 (DIN 66399). דוגמאות ליישום: א. גריטת מצע אחסון מידע אשר הכיל מידע רגיש - בהתאם לרמת DIN 3 ב. גריטת מצע אחסון מידע אשר הכיל מידע חסוי - בהתאם לרמת DIN 4 גריטת מצע אחסון מידע מסוג SSD אשר הכיל מידע רגיש/חסוי - בהתאם לרמת DIN 5	
מדיניות גיבויים		
.25	מומלץ כי הארגון יוודא כי מדיניות הגיבויים עומדת בדרישות תוכנית המשכיות עסקית של הארגון.	
.26	מומלץ כי הארגון יוודא כי מדיניות הגיבויים (מוכרת גם בשם "משטר גיבויים") כוללת התייחסות לנושאים הבאים: א. סוג המידע המגובה. לדוגמה: - קבצים (Files)	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	- בסיסי נתונים רלציוניים (RDBMS) - בסיסי נתונים לא רלציוניים (NoSQL) - אובייקטים של שירותי ספרייה (Directory Services) - הגדרות תצורה (System Configurations), לרבות ציוד תקשורת ואמצעי אבטחת מידע וסייבר - דיסקים וירטואליים (Virtual Disks) - מערך אחסון בתור (Queue Storage) - קושחה (Firmware) - Images ארגוניים - מטה דאטה (Metadata) - קוד מקור (Source Code) - מערכת הפעלה (Operating Systems) - קונטיינרים (Containers) - לוגיקה של בקרים מתוכנתים (PLC) ב. שיטת הגיבוי רצויה. להרחבה ראו נספח 3'. ג. צורות אחסון (Storage Media) /סוגי מדיה. להרחבה ראו נספח 4'. ד. זמינות רצויה של אחסון הגיבוי. להרחבה ראו נספח 5'. ה. גישה רצויה לגיבוי "מידע חי". להרחבה ראו נספח 6'.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	ו. בדיקות הגיבויים, ביצוע שחזורים יזומים, ביצוע תרגילי שחזור שנתי. להרחבה ראו נספח 7'. ז. התראות ודיווחים. להרחבה ראו נספח 8'. ח. אורך החיים לשמירה על המידע (Data Retention). ט. אורך החיים למחיקת מידע (Data Purging). י. מספר העתקי מידע רצויים. יא. תדירות הגיבויים. יב. מיקום פיזי/לוגי אחסון הגיבוי. יג. מימוש עקרון "חוק 3/2/1" - כינוי לעקרון בו הארגון מחזיק שלושה עותקי מידע, שני סוגי מדיה, אתר חיצוני אחד. יד. קיומה של יכולת לשחזור נכס הסייבר לדגם חומרה שונה מהמקור. טו. קיומה של יכולת לשחזור נכס הסייבר לדגם חומרה מיצרן אחר מאשר המקור. נספח 9 - מכיל מדיניות בסיסית גיבוי לדוגמה	
27.	מומלץ כי הארגון יקבל באופן עתי חוות דעת צד-שלישי להתאמת מדיניות הגיבויים לצרכיו. מומלץ להסתייע לכל הפחות בגורמי המקצוע הבאים: א. ממונה המשכיות עסקית בארגון. ב. יועץ המשכיות עסקית צד-שלישי. ג. מומחה גיבויים צד-שלישי.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	ד. יועץ הגנת סייבר צד-שלישי.	
28.	מומלץ כי הארגון יוודא כי תוכנת הגיבוי מכילה רכיב אופטימיזציה לשליטה ובקרה על משימות הגיבוי/השחזור, וזאת במטרה להקטין את תקורות הניהול למינימום האפשרי.	
דגשים לעבודה עם ענן ציבורי		
29.	מומלץ כי הארגון יוודא שאחסון המידע מתבצע באתרים אשר עונים לדרישות החוק, רגולציה, דרישות חוזיות וצרכים עסקיים.	
30.	מומלץ כי הארגון יוודא בעת עבודה במודל שירות SaaS כי: א. מדיניות הגיבויים של הספק עונה לצרכי הארגון, ומעוגנת משפטית. ב. מתבצע הליך העברת העתק גיבוי באופן עתי לחצרות הארגון.	
31.	מומלץ כי הארגון יוודא בעת עבודה במודל שירות IaaS\PaaS כי: א. העתק הגיבוי מועתק באופן עתי לסביבה מבודלת בענן. ב. גורם אשר השיג גישה לחשבונות הניהול של הארגון לענן אינו מסוגל לבצע שינויים/מחיקה לגיבויים.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	ג. ישנה אכיפה לנושא אורך החיים לשמירה על המידע (Data Retention). ד. ישנה אכיפה לנושא אורך החיים למחיקת מידע (Data Purging).	
32.	מומלץ כי הארגון יוודא כי ספק הענן עושה שימוש בפורמט פתוח ומקובל לגיבויים, כך שניתן יהיה לבצע שחזור של המידע לתשתית של ספק אחר או לנכס סייבר שונה מהמקור.	
33.	מומלץ כי הארגון יוודא כי כאשר הגיבוי נעשה לענן, הדבר כולל שינוי פורמט למידע. דוגמא ליישום: גיבוי של קובץ מסמכים למדיית אחסון בענן ציבורי מסוג "אחסון אובייקטים" (Object Storage)	
התמודדות עם נוזקות (Malware)		
34.	מומלץ כי הארגון יוודא בטרם העתקת הקבצים ליעד (דוגמת מדיית האחסון/הגיבוי או שרת שיש לשחזרו) כי המידע אינו מכיל נוזקות וזאת ע"י שימוש באמצעים מקובלים. בכלל זה, יש לעשות שימוש בעקרון מידרוג (Staging) לשם ביצוע הבדיקה באזור מבודל.	
35.	מומלץ כי הארגון יוודא כי מערך הגיבוי אינו מגבה ומאחסן סוגי קבצים אשר אינם מותרים בהתאם למדיניות הארגון. דוגמא ליישום: שימוש במנגנון File Screening	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.36	מומלץ כי הארגון יוודא כי מערך הגיבוי כולל "נתיך" (Fuse) המאפשר ניתוק של מערך הגיבוי מהרשת במקרה של אירוע סייבר/נחשול סייבר.	
.37	מומלץ כי הארגון יוודא כי מערך הגיבוי כולל מימוש של בידול לוגי (Air-Gap), כך שיתקיים מצב של ניתוק לוגי בין סביבת הגיבוי בייצור, אל מול עותק הגיבוי באתר החלופי (DR).	
זמינות מערך הגיבוי		
.38	מומלץ כי הארגון יוודא כי ברשותו מערך גיבוי חלופי ובלתי תלוי באתר החלופי (DR).	
.39	מומלץ כי הארגון יוודא כי ברשותו יתירות לרכיבי ליבה במערך הגיבוי, דוגמת שרת הניהול. דוגמא ליישום: שימוש בתצורת HA (High Availability) הכולל שרת Primary ו-Follower	
.40	מומלץ כי הארגון יוודא כי בעת החלפת מערך הגיבוי, מערך הגיבוי הישן יהיה זמין ותקין וזאת עד לסיום הצורך העסקי בשחזור מידע היסטורי.	
.41	מומלץ כי הארגון יבחן שימוש בטכנולוגיות מקובלות המעלות את רמת הזמינות והיתירות, תוך צמצום קיומה של נקודת כשל יחידה. בכלל זה, יש לשים דגש לנושא מדיית האחסון. דוגמא ליישום: שימוש בפתרון גיבוי מבוסס Raid תוכנתי מסוג EC (Erasure Coding) המאפשר רמת זמינות גבוהה,	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	ויצירת מספר עותקים במערך הגיבוי עבור המידע המגובה.	
יתירות כוח אדם מקצועי		
42.	מומלץ כי הארגון יוודא כי ברשותו יתירות לכוח האדם המקצועי המתפעל את מערך הגיבוי.	
43.	מומלץ כי הארגון יוודא כי כוח האדם המקצועי המתפעל את מערך הגיבוי זמין על בסיס 24/7.	
דרישות ארכיטקטורה		
44.	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. בהתאם ל"ארכיטקטורה טיפוסית של מערך גיבוי נתונים" לעיל, כל רכיב יותקן ב-VLAN ייעודי. ב. תעבורת הגיבוי תעבור על-גבי רשת ייעודית (OOB), כאשר לכל נכס סייבר מגובה יוקצה כרטיס רשת ייעודי לטובת העניין. ג. יעשה שימוש ב-Microsegmentation	
45.	מומלץ כי הארגון יישם עקרונות מקובלים למידור רשתי (Network Segregation) - אכיפת כללי גישה בין יעדי הגנה החולקים רשת משותפת. יש לתת את הדעת לסינון	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	תעבורה בין המכונות הווירטואליות (East-West Traffic) אשר אינה עוברת דרך ה-FW הרשתי. דוגמאות ליישום: א. שימוש ב-FW רשתי. ב. שימוש ב-Distributed FW	
.46	מומלץ כי הארגון יוודא כי מערך הגיבוי אינו עושה שימוש בפורטים דינמיים (Dynamic Ports).	
.47	מומלץ כי הארגון יוודא כי תהליך הגיבוי עושה שימוש בעקרון משיכה (Pull), כך ששרת ניהול הגיבוי הוא זה שפונה ללקוחות, ולא ההיפך. יש לוודא באופן עתי כי הגדרת תצורה זו לא השתנתה עקב תקלה או עקב סיבה אחרת.	
.48	מומלץ כי הארגון יוודא כי שעון רכיבי מערך הגיבוי מסונכרנים מול שעון זמן מהימן, וזאת תוך מניעת אפשרות לניצול לרעה של ערוץ זה (דוגמת התחזות לשעון זמן מהימן).	
.49	מומלץ כי הארגון יוודא כי גישה לניהול מערך הגיבוי תתבצע דרך שרת מתווך (Jump Server).	
אבטחת תהליך הזדהות (Authentication) משתמשים		
.50	מומלץ כי הארגון יוודא כי גישה מחייבת השלמה מוצלחת של אימות רב-גורמי (MFA), וזאת לצד גישה בהתאם לכתובת IP הנמצאת ברשימה לבנה.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.51	מומלץ כי הארגון יוודא כי הוא נועל את חשבונות מערך הגיבוי לאחר X ניסיונות גישה לא מורשים.	
.52	מומלץ כי הארגון יוודא כי גורמי תפעול אינם יודעים את סיסמת החשבונות האפליקטיביים בהם מערך הגיבוי עושה שימוש, וכי תהליך החלפת הסיסמה של חשבונות אלו נעשה ללא מעורבות יד-אדם. דוגמאות ליישום: א. שימוש ביכולות המובנות בשירותי הספרייה הארגונית. ב. שימוש ב-PIM (Privileged Identity Management)	
.53	מומלץ כי הארגון יוודא כי שמות החשבונות האנושיים/האפליקטיביים שונים מאלו של ברירת המחדל, וכי הם אינם חושפים מידע אודות זהות/מאפייני המערכת.	
.54	מומלץ כי הארגון יגביל את מספר הפעילויות (Sessions) המותרות בו-זמנית של משתמש בודד. ככלל, אין לאפשר יותר מפעילות יחידה בזמן נתון.	
.55	מומלץ כי הארגון יוודא כי שרתי מערך הגיבוי לא יקושרו לדומיין (Domain).	
.56	מומלץ כי הארגון יוודא כי ניהול מערך הגיבוי יעשה באמצעות חשבונות מקומיים בלבד, ולא חשבונות דומיין (Domain) ו/או חשבונות המאוחסנים בשירותי ספריה (Directory Services). יש לשים דגש לנושא שרת ניהול הגיבוי (BS) ושרת ניהול המדיה (MS).	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
אבטחת תהליך בקרת גישה / ניהול הרשאות (Authorization)		
.57	מומלץ כי הארגון יוודא כי שינוי מדיניות גיבוי פעילה מחייב אישור סימולטאני של שני גורמים בלתי-תלויים (Dual Control).	
.58	מומלץ כי הארגון יוודא כי ישנה הפרדת סמכויות בין המשתמשים במערך הגיבוי (SOD - Segregation of Duties). לדוגמה: משתמש פלוני יוכל להוסיף נכס סייבר למערך הגיבוי, ואילו משתמש אלמוני יחיל את ההגדרות בפועל.	
.59	מומלץ כי הארגון יוודא כי מתן גישה למערך הגיבוי יתבצע בהתאם לעקרון הצורך לדעת (Need to Know).	
מהימנות תעסוקתית		
.60	מומלץ כי הארגון יוודא כי משתמשים בעלי נגישות למערך הגיבוי יעברו בחינת מהימנות מעמיקה, וזאת לצד בדיקה בתדירות גבוהה יותר. הסיבה לכך נובעת מהנגישות הגבוהה של משתמשים לצבר מידע.	
דרישות קריפטוגרפיה		
.61	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.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.62	מומלץ כי הארגון יוודא כי שינוע קובץ יעשה על גבי תווך מוצפן. דוגמא ליישום: שימוש ב-TLS v1.3	
.63	מומלץ כי הארגון יוודא כי תהליך חילול מפתחות ההצפנה הוא בעל אנטרופיה גבוהה, המונעת אפשרות לניחוש מפתח ההצפנה או השפעה על תהליך החילול שלו.	
.64	מומלץ כי הארגון יוודא כי במסגרת ביצוע תהליכים קריפטוגרפים לא נחשף מידע ערכי בערוץ-צד (Side Channel). דוגמא ליישום: הוספת "רעש לבן" לתהליך החילול. להלן דוגמאות של ערוצי-צד: א. רעש מאוורר ב. נורת חיווי בדיסק ג. פלט אלקטרומגנטי	
.65	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). ככלל יש להעדיף לעשות שימוש בהתקני HSM העומדים בדרישות תקנים מקובלים, דוגמת Common Criteria EAL 4 or Higher	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.66	מומלץ כי הארגון יוודא כי האלגוריתמים הקריפטוגרפים עומדים בדרישות תקן FIPS 140-2 Level 3 ומעלה.	
.67	מומלץ כי הארגון יוודא כי אינטגרציה עם KMS חיצוני תעשה באמצעות שימוש בפרוטוקול KMIP מקובל.	
.68	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	
.69	מומלץ כי הארגון יוודא כי גם במקרה שתוקף השיג גישה לסיסמת המשתמש, הוא לא יוכל לאחזרה. דוגמא ליישום: שימוש ב-Hash + Salt	
.70	מומלץ כי הארגון יוודא כי מערך הגיבוי עושה שימוש במנגנונים קריפטוגרפים על מנת להגן על שלמות רשומות וכלי הבקרה.	
.71	מומלץ כי הארגון יוודא כי בעת ניסיון לאחזור סיסמה, כוח העיבוד אשר יידרש להשקיע יעלה באופן ליניארי.	
.72	מומלץ כי הארגון יוודא כי האלגוריתמים הקריפטוגרפים במערך הגיבוי מספקים חסינות בפני מחשוב קוואנטי.	
.73	מומלץ כי הארגון יוודא כי מערך הגיבוי מבוסס על עקרונות מקובלים בהנדסת תוכנה, דוגמת אַטוֹמִיוּת, עִקְבִיוּת, בִּידוּד וְעֶמִידוּת (ACID - Atomicity, Consistency, Isolation, Durability).	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
עדכוני אבטחה (פאצ'ים) וניהול גרסאות		
74.	מומלץ כי הארגון יוודא החלת עדכוני אבטחה בהתאם למדיניות הארגון. יש לתת את הדעת לנושא החלת עדכוני האבטחה לסוכן (Agent) בנכסי הסייבר.	
75.	מומלץ כי הארגון יוודא שדרוג לגרסה עדכנית של מערך הגיבוי, וזאת לשם שמירה על תאימות למערכות הפעלה ואפליקציות עדכניות. יש לתת את הדעת לנושא שדרוג סוכן (Agent) בנכסי הסייבר.	
בדיקות לביצוע לאחר ביצוע שחזור		
76.	מומלץ כי הארגון יוודא כי לאחר ביצוע שחזור רמת האבטחה של נכס הסייבר/המידע נשמרת. בכלל זה, יש להתייחס לנושאים מקובלים דוגמת: א. הרשאות גישה (לרבות ביצוע השוואה ביחס למצב ההרשאות בעבר). ב. לא התווספו קבצים/תכנים נוספים שמקורם לא ידוע. ג. הקשחת מערכת (System Hardening). ד. תקינות אמצעי האבטחה (אנטי-וירוס וכד'). ה. אתחול בטוח (Secure Boot).	
77.	מומלץ כי הארגון יוודא כי לאחר ביצוע שחזור, הגדרות התצורה של נכס הסייבר חוזרות למצב הרצוי.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.78	מומלץ כי הארגון יוודא כי לאחר ביצוע שחזור, הפונקציונאליות העסקית פועלת כמצופה. בכלל זה יש לקבל את אישור הגורם המקצועי לתקינות לאחר השלמת סט בדיקות שהוגדר מבעוד מועד.	
.79	מומלץ כי הארגון יוודא כי לאחר ביצוע שחזור מידע כי: א. לא בוצע שחזור למידע שמחיקתו נדרשת בהתאם לדרישות חוק, רגולציה, דרישות עסקיות וצרכים עסקיים. ב. התקבל אישור מגורם עסקי רלוונטי בארגון לעמידה בדרישה לעיל.	
ביקורות		
.80	מומלץ כי הארגון יוודא באופן עתי כי אין במערך הגיבוי חשבונות משתמשים שאינם נדרשים לעבודה שוטפת. בכלל זה, יש לבצע הבחנה בין חשבונות משתמשים רגילים, לחשבונות משתמשים חזקים.	
.81	מומלץ כי הארגון יוודא באופן עתי כי קיבולת וביצועי מערך הגיבויים עונה לצרכיו.	
שרשרת אספקה		
.82	מומלץ כי הארגון יוודא כי ספקי השירות הרלוונטיים עומדים בדרישות מתודת שרשרת האספקה של המערך [3].	
תיעוד וניטור		

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

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.83	מומלץ כי הארגון יוודא כי מערך הגיבוי מבצע תיעוד ביומן רישום אוטומטי וייעודי (רישום Log) כל יצירה, שינוי, אפשור, ניטרול והסרה של חשבון משתמש.	
.84	מומלץ כי הארגון יוודא כי מערך הגיבוי מבצע תיעוד ביומן רישום אוטומטי וייעודי (רישום Log) מתן הרשאה, שינוי, אפשור, והסרת הרשאה.	
.85	מומלץ כי הארגון יוודא כי מערך הגיבוי מבצע תיעוד ביומן רישום אוטומטי וייעודי (רישום Log) של פעולות יצירה, קריאה, עדכון ומחיקה (CRUD - Create, Read, Update, and Delete).	
.86	מומלץ כי הארגון יוודא כי מערך הגיבוי כולל מנגנון לשליחת התראה במידה של הפסקת כתיבת נתונים ללוגים/ייצור לוגים.	
.87	מומלץ כי הארגון יוודא כי מערך הגיבוי כולל מנגנון המאפשר ניטור פעילות חשבונות לזיהוי שימוש חריג, ודיווח על שימוש חריג לבעלי התפקידים המתאימים. במקרה של העתק תמיכה מובנית, יש לספק בקרה מפצה.	
.88	מומלץ כי הארגון יוודא כי מערך הגיבוי יקושר למערכת הניטור הארגונית (SIEM). בכלל זה יש לתעד ונהל אירועים מקובלים, דוגמת: א. הוספה/הסרה של נכס סייבר למערך הגיבוי. ב. הוספה/הסרה של לקוח למערך הגיבוי.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	ג. הוספה/הסרה/שינוי של מדיניות גיבוי כללית, ופר לקוח. ד. הוספה/הסרה/שינוי של מדיית אחסון ומאפייניה. ה. הוספה/הסרה/שינוי חשבון משתמש במערך הגיבוי (לרבות חשבון אפליקטיבי). ו. הוספה/הסרה/שינוי הרשאות חשבון משתמש במערך הגיבוי (לרבות חשבון אפליקטיבי). ז. הוספה/הסרה/שינוי מפתח הצפנה. ח. אי הצלחה בהשלמת משימת גיבוי. ט. גילוי וזיהוי נוזקות במסגרת תהליך הגיבוי/השחזור. י. אנומליה וחריג חשוד טעות (Outlier) במשימות גיבוי וקבצים - דוגמת נפחי גיבוי שונים בין גיבוי עבר להווה, התארכות/התקצרות זמן גיבוי, שינוי בתדירות ביצוע משימות הגיבוי, שונות בין קבצים שגובו בעבר לקבצים בהווה (סיומות קבצים, גודל, אנטרופיה, הרשאות גישה וכד'). יא. ביצוע פעולת שחזור. יב. שחזור מידע שלא ליעד המקורי.	

טבלה 4: המלצות ליישום - שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור

יש לתת את הדעת כי במקרים מסוימים הארגון עשוי להידרש לעשות שימוש במערכות נלוות לשם ביצוע הגיבוי. כך לדוגמה, לשם גיבוי הגדרות תצורה הארגון עשוי להידרש לעשות שימוש ב-SCM\CMDB (Secure Configuration Management). לאחר מכן, מערך הגיבוי המרכזי יוכל לגבות את הגדרות התצורה ממערכת זו, וזאת ללא צורך בביצוע הפעולה מול כל נכס סייבר באופן עצמאי.

ישנם מקרים בהם ניתן לעשות שימוש בתמונת מצב (Snapshot) במערך האחסון או בסביבה הווירטואלית כמענה ראשוני לשחזור מידע. עם זאת, שיטת עבודה זו אינה מספקת מענה שלם, והיא כפופה למגבלות הגנת סייבר ותפעול שונות.

7. נספחים (Appendixes)

פרק זה מכיל את רשימת הנספחים הנלווים למסמך זה.

נספח 1 - שילוב עקרונות הגנת סייבר בתהליכי גיבוי ושחזור

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. הטכניון
ב. אוניברסיטת חיפה
ג. טריפל סי מחשוב ענן בע"מ
ד. קומוולט סיסטמס (ישראל) בע"מ
ה. אינוקום בע"מ
ו. Veeam Software
ז. עו"ד עינבר בן-ציון רגרמן
ח. מר אור שלום (סייב-סק)
ט. מר אורן ויסמן

נספח 2 - מושגים עיקריים בעולם הגיבוי והשחזור

מטרת הנספח

הצגת מושגים עיקריים בעולם הגיבוי והשחזור, וזאת במטרה ליצור שפה משותפת עם הקוראים.

א. אימות גיבוי (Backup validation) - התהליך שבאמצעותו יכול המפעיל לקבל מתוכנת הגיבוי משוב על הצלחת גיבוי המידע. ראוי לציין כי למרות קיומה של יכולת זו, לא ניתן להסתמך על יכולת זו באופן בלעדי.

ב. בדיקת כפילויות (De-duplication[4]) - שיטה המונעת גיבוי חוזר של מידע קיים, דבר המאפשר השגת חסכון בנפח אחסון, לצד קיצור זמן הגיבוי/השחזור.

ג. גיבוי - גיבוי הוא עותק של המידע הדיגיטלי אשר מאוחסן במקום אחר מאשר בנכס הסייבר המקורי בו המידע מאוחסן. הגדרה חלופית לפי האקדמיה ללשון[5]: שמירת עותק של קובצי מחשב, יישומים ותוכנות למקרה של אובדן או תקלה תמיכה ועמידה לצידו של אדם או של ארגון וכדומה בשעת הצורך.

ד. גיבוי מבוסס פרוטוקול NDMP - מערכות אחסון מסוימות מתאפיינות ביכולתן לגבות ולשחזר את החומר המאוחסן בהן בצורה ישירה ממערכת האחסון ישירות לספריית הגיבוי (או יעד אחר), וזאת ללא שימוש במשאבי הרשת והשרתים, ותוך השתלבות בתוכנת הגיבוי הארגונית הקיימת.

ה. זמן היעד להתאוששות (RTO - Recovery Time Objective) - טווח הזמן הנדרש לטובת הפעלה מחדש של הפעילות העסקית. מקובל כי ערך זה נגזר מתוכנית ההמשכיות העסקית (BCP) של הארגון.

ו. "חוק 3/2/1" - כינוי לעקרון בו הארגון מחזיק שלושה עותקי מידע, שני סוגי מדיה, אתר חיצוני אחד.

ז. מידרוג (Staging) - העברת המידע המגובה/המשוחזר למדיית אחסון זמנית ("ביניים"). ביצוע מידרוג מאפשר שילוב בדיקות הגנת סייבר בתהליך ו/או מתן מענה לפערי ביצועים בין רכיבים המעורבים בתהליך.

ח. ספריית גיבוי (Tape Library) - רכיב חומרה המאפשר גיבוי של המידע למדיה מסוג קלטת פיזית.

ט. ספריית גיבוי וירטואלית (VTL - Virtual Tape Library) - מערך אחסון המדמה

---

[4] לעיתים נעשה שימוש בקיצור DEDUP

[5] על המילה גִּבּוּי
https://hebrew-academy.org.il/keyword/%D7%92%D6%BC%D6%B4%D7%91%D6%BC%D7%95%D6%BC%D7%99

לתוכנת גיבוי מסורתית את קיומה של ספרית גיבוי פיזית. יתרון שיטה זו ביחס לספריה פיזית מסורתית הינו קצב הגיבוי/השחזור הגבוה.

י. נקודת השחזור הרצויה למידע (RPO - Recovery Point Objective) - טווח הזמן שהצטבר בו מידע שאותו ניתן לאבד בעת אירוע סייבר או תקלה תפעולית. מקובל כי ערך זה נגזר מתוכנית ההמשכיות העסקית (BCP) של הארגון.

יא. תכונת כתיבה אחת, קריאה מרובה (WORM - Write Once Read Many) - תכונה המונעת אפשרות לשכתוב או שינוי מידע אשר נכתב על-גבי מדיית אחסון.

נספח 3 - שיטות גיבוי עיקריות

מטרת הנספח

נספח זה סוקר שיטות גיבוי עיקריות.

מס'	שם השיטה	תיאור	הערות
1.	העתקת מידע לא מובנה (Unstructured)	העתקה של מידע ממדיית אחסון מקור, למדיית גיבוי אחרת. שיטה זו מתאימה בד"כ לגיבוי מזדמן של נפחי מידע קטנים.	
2.	גיבוי מלא (Full Backup)	גיבוי מלא הוא גיבוי של כל המידע הדיגיטלי שהוגדר. שחזור המידע לנקודת זמן מסוימת מצריך שחזור של הגיבוי המלא האחרון שנעשה לנקודת הזמן הרצויה. במקרים מסוימים יתכן שבנוסף יעלה הצורך לבצע שחזור של גיבוי השינויים האחרון, או לחילופין, שחזור של כל הגיבויים המצטברים עד לנקודת הזמן הרצויה. סוג גיבוי זה מבטיח רמת ביטחון גבוהה שניתן יהיה לשחזר את המידע הדרוש. עם זאת, גיבוי זה סובל ממספר מגבלות אשר הבולטים ביניהם הינם הזמן הארוך הנדרש לשחזור המידע, והדרישה הגבוהה לנפח אחסון.	
3.	גיבוי שינויים - (Differential Backup)	גיבוי שינויים הוא גיבוי של כל שינוי שבוצע במידע מאז הגיבוי המלא האחרון.	
4.	גיבוי מצטבר (Incremental Backup)	גיבוי מצטבר הוא גיבוי של שינויים במידע מאז הגיבוי המצטבר האחרון או הגיבוי המלא האחרון. גיבוי זה סובל ממספר מגבלות, אשר הבולטים ביניהם הינם הזמן הארוך הנדרש לשחזור המידע והתלות בתקינות גרסאות מצטברות לשם חזרה לנקודת זמן רצויה. לדוגמה; ארגון ביצע גיבוי מלא ביום ראשון, ובימים שני, שלישי, רביעי וחמישי ביצע גיבוי	

		מצטבר בלבד. במקרה של צורך לחזרה לגיבוי הנכון ליום רביעי, הארגון יצטרך להשלים שחזור של הגיבוי המלא, וכן שחזור של גיבוי מצטבר אשר מקורו מהימים שני, שלישי ורביעי. במקרה של תקלה טכנית בגיבוי מצטבר מיום שלישי, הארגון יוכל לשחזר מידע הנכון ליום שני בלבד.	
5.	גיבוי רציף ומתמשך (Continuous Backup)	גיבוי רציף ומתמשך המאפשר גיבוי של מידע בסמיכות גבוהה לתאריך היצירה/השינוי שלו.	
6.	גיבוי סינטטי (Synthetic Backup)	גיבוי סינטטי מאפשר יצור של גרסה עצמאית של גיבוי מלא (בד"כ), וזאת על סמך גיבוי היסטורי (בד"כ מלא ומצטבר). יתרונות בולטים של שיטה זו הינם החסכון במשאבי מחשוב ושטח אחסון. חסרונות בולטים של שיטה זו עשויים להיות פגיעות גבוהה יותר לאירוע סייבר או לתקלה תפעולית. יצוין כי חלק מהיצרנים מציעים יכולות נוספות בפתרון מטעמם, דוגמת שמירה על יכולת לחזור לגרסאות גיבוי מצטבר קודמים.	

טבלה 5: שיטות גיבוי עיקריות

נספח 4 - צורות אחסון (Storage Media) /סוגי מדיה מקובלות

מטרת הנספח

סקירת צורות אחסון (Storage Media) /סוגי מדיה מקובלות.

מס'	צורת האחסון	תאימות לעבודה בארגון	זמן גיבוי/שחזור	אמינות לאורך זמן	תמיכה ב-WORM	עלות
1.	סרט מגנטי (קלטות)	כן	גבוה	נמוכה	כן	בינונית
2.	דיסק קשיח	למקרים נקודתיים	בינוני	נמוכה	לא	נמוכה
3.	מערך אחסון שריד (RAID)[6]	כן	נמוך	בינונית-גבוהה (תלוי מימוש)	תלוי מימוש	(בינונית נמוכה יחסית בנפחים גדולים)
4.	דיסק אופטי	למקרים נקודתיים	גבוה	בינונית	כן	נמוכה מאוד
5.	התקן נייד (דוגמת DOK)	למקרים נקודתיים	בינוני	בינונית (תלוי מימוש)	לא	נמוכה מאוד
6.	אחסון אובייקטים	כן	נמוך-בינוני	בינונית-גבוהה	תלוי מימוש[7]	נמוכה-בינונית

[6] חלק מיצרני פתרונות האחסון מציעים כיום תמיכה באחסון אובייקטים (Object Storage)

[7] מקובל לראות כי ענן ציבורי מציע תצורות עבודה מגוונות, דוגמת:
א. Standard Tier – מיועד לשימוש כללי, כאשר נדרשת גישה בזמן אמת למידע
ב. Infrequent Access – מיועד לשימוש כאשר הגישה למידע משתנה או בלתי ידועה
ג. Archive – מיועד לגיבויים ולאחסון מידע ארכיוני, כאשר זמן האחסון המינימלי הוא 90 יום
ד. Long Term Archive – מיועד לאחסון מידע ארכיוני לזמן רב, כאשר זמן האחסון המינימלי הוא 180 יום
קרדיט למרכז החישובים הבינאוניברסיטאי (מחב"א) ומר אייל אסטרין, מקור: כיצד לבחור בשירות אחסון מנוהל בענן https://www.iucc.ac.il/he/blog/select-cloud-storage /

	Object) (Storage			(תלוי מימוש)	
7.	שירותי גיבוי מרחוק	כן	נמוך-בינוני (בד"כ תלוי רוחב-פס)	בינונית-גבוהה (תלוי מימוש)	תלוי מימוש	נמוכה-בינונית

טבלה 6: צורות אחסון (Storage Media) /סוגי מדיה מקובלות

נספח 5 - מודלים מקובלים לבחינת זמינות אחסון הגיבוי

מטרת הנספח

סקירת מודלים מקובלים לבחינת זמינות אחסון הגיבוי.

מס'	זמינות האחסון	תיאור	רמת עמידות בפני אירוע סייבר	מסגרת הזמן לתחילת ביצוע פעולת גיבוי/שחזור
1.	מקוון (On-Line)	הגישה לאחסון זמינה באופן קבוע למפעיל	נמוכה מאוד	שניות (בד"כ)
2.	מקורב למקוון (Near On-Line)	המפעיל יכול לגשת לאחסון בכפוף להשלמת "זמן גישה"	נמוכה	שניות עד דקות בודדות
3.	לא מקוון (Off-Line)	התערבות פיזית או לוגית של המפעיל חיונית לשם ביצוע פעולת הגישה לאחסון	בינונית - התערבות לוגית (דוגמת בחירה מהי המדיה שיש לגשת אליה) בינונית-גבוהה - התערבות פיזית (דוגמת הוצאת קלטת מכספת פיזית, והכנסתה לספרית גיבוי)	דקות עד שעה
4.	מחוץ לאתר (Off-Site)	מדיית האחסון מאוחסנת פיזית מחוץ למתחם שבו מאוחסן נכס הסייבר.	גבוהה מאוד (מתאימה גם למקרי קיצון דוגמת שרפה במתחם)	שעות/ימים

טבלה 7: מודלים מקובלים לבחינת זמינות אחסון הגיבוי

נספח 6 - גישות מקובלות לגיבוי "מידע חי"

מטרת הנספח

סקירת גישות מקובלות לגיבוי "מידע חי".

מס'	זמינות האחסון	תיאור
1.	גיבוי קר (Cold Backup)	גישה שבה מסד הנתונים אינו זמין למתן שירות ללקוחות בזמן הגיבוי
2.	גיבוי חם (Hot Backup)	גישה שבה מסד הנתונים זמין למתן שירות ללקוחות בזמן הגיבוי
3.	גיבוי קבצים פתוחים (Open Files Backup)	גישה שבה מתבצע גיבוי לקבצים פתוחים. במקרה זה תוכנת הגיבוי עשויה לבצע את הגיבוי בשלב מאוחר יותר כאשר הקובץ "סגור" או ליצור תמונת מראה (Snapshot) שלו
4.	תמונת מראה (Snapshot)	המימוש של גישה זו מגוון, ותלוי יצרן. להלן סקירה של שני מימושים שכיחים: א. גישת שרשור "תמונת מצב" - בגישה זו ישנה תלות בין תמונת מצב חדשה, לתמונת מצב ישנה (בדומה ל"גיבוי מצטבר"). ב. גישה ללא שרשור "תמונת מצב" - בגישה זו אין תלות בין תמונת מצב חדשה, לתמונת מצב ישנה (בדומה ל"גיבוי שינויים").

טבלה 8: גישות מקובלות לגיבוי "מידע חי"

נספח 7 - בדיקות הגיבויים, ביצוע שחזורים יזומים, ביצוע תרגילי שחזור שנתי

מטרת הנספח

סקירת בדיקות הגיבויים, ביצוע שחזורים יזומים, ביצוע תרגילי שחזור שנתי.

מס'	שם הבדיקה	אופן ביצוע הבדיקה	תדירות הבדיקה מומלצת
.1	בדיקת גיבויים	בדיקת תקינות הגיבוי ברמת התהליכים העסקיים, בדיקת הלוגים, אימות גיבוי (Backup validation), בדיקת הודעות השגיאה, מעקב אחר נפחי דיסק ושטחי אחסון.	יומית
.2	בדיקה פיזית-ויזואלית	בדיקה פיזית-ויזואלית של התקני הגיבוי, לדים וכו'.	יומית
.3	בדיקת שחזור יזומה של פריט מידע	בדיקת שחזור יזומה של פריטי מידע מתוך שרת, למיקום אלטרנטיבי או לספרייה חדשה במיקום המקורי. בהתאם לנוהל המדיניות הארגוני.	שנתית
.4	בדיקת שחזור יזומה של שרת	בדיקת שחזור יזומה של שרת אקראי בצורה מלאה למיקום אלטרנטיבי. בהתאם לנוהל המדיניות הארגוני.	שנתית
.5	בדיקת שחזור יזומה של מערכת בסביבת ייצור	בדיקת שחזור יזומה של מערכת הייצור למיקום אלטרנטיבי. בהתאם לנוהל המדיניות הארגוני.	שנתית
.6	תרגילים שנתיים	כחלק מתוכנית העבודה השנתית, יש לבצע תרגילים שנועדו לבחון את תפקוד המערכות בעתות חירום. בהתאם לנוהל המדיניות הארגוני.	שנתית

טבלה 9: בדיקות הגיבויים, ביצוע שחזורים יזומים, ביצוע תרגילי שחזור שנתי

נספח 8 - התראות ודיווחים

מטרת הנספח
סקירת התראות ודיווחים.

מס'	תיאור הדוח	תדירות הדוח	הגורם המדווח
1.	**הגדרת התראות בדוא"ל** יש להגדיר התראות לגורמים הרלוונטיים, אודות כישלונות בתהליכי הגיבוי.	שוטף	
2.	**דו"ח סטטוס גיבויים יומי** הדו"ח יכלול דיווח אודות הגיבויים היומיים בציון תאריך ושעת התחלת הגיבוי, תאריך ושעת סיום הגיבוי, יעד הגיבוי, סטטוס הגיבוי, נפח המידע המגובה. הדו"ח היומי יכלול את פעילות הגיבוי של יום האתמול. במידה והגיבוי נכשל, יש לכלול את הודעת השגיאה ומה נעשה לתיקון.	יומי	
3.	**דו"ח סטטוס גיבויים שבועי** הדו"ח יכלול דיווח אודות הגיבויים השבועיים בציון תאריך ושעת התחלת הגיבוי, תאריך ושעת סיום הגיבוי, יעד הגיבוי, סטטוס הגיבוי, נפח המידע המגובה. הדו"ח השבועי יכלול את פעילות הגיבוי של סוף השבוע האחרון. במידה והגיבוי נכשל, יש לכלול את הודעת השגיאה ומה נעשה לתיקון.	שבועי	
4.	**דו"ח סטטוס גיבויים חודשי, שנתי** הדו"ח יכלול דיווח אודות הגיבויים החודשיים \ שנתיים בציון תאריך ושעת התחלת הגיבוי, תאריך ושעת סיום הגיבוי, יעד הגיבוי, סטטוס הגיבוי, נפח המידע המגובה. הדו"ח החודשי \ שנתי יכלול את פעילות הגיבוי של סוף החודש \ סוף השנה. במידה והגיבוי נכשל, יש לכלול את הודעת השגיאה ומה נעשה לתיקון.	חודשי	

.5	**דו"ח שחזורים** לאחר כל שחזור (שבועי, חודשי, שנתי) יוגש דו"ח בציון מבצע השחזור, תאריך ושעת השחזור, פרטי המידע ששוחזרו, מיקום השחזור, סטטוס השחזור. במידה והשחזור נכשל, יש לכלול את הודעת השגיאה ומה נעשה לתיקון.	שבועי, חודשי, שנתי ובתוך 24 שעות מסיום השחזור.	
.6	**דו"ח מגמות סטטיסטי** דו"ח רבעוני לגבי מגמות גידול המידע במערכת במספרים ובגרף.	בסוף כל רבעון	
.7	**דו"ח אירועים חריגים** דו"ח אירועים חריגים, דוגמת: א. גודל חשוד של קבצי גיבוי אינקרמנטליים יחסית לממוצע גודל הגיבוי האינקרמנטלי בשלושה עד חמישה ימים שלפני כן. ב. שינוי בסיומות קבצים ביחס לגיבויי עבר. ג. שינוי ברמת האנטרופיה של הקבצים ביחס לגיבויי עבר.		

טבלה 10: התראות ודיווחים

נספח 9 - מדיניות גיבוי לדוגמה

שרתים פיזיים:

סוג הגיבוי	מספר העתקים	מספר מדיות	עם עותק מרוחק	תדירות	זמן שמירה	זמן ביצוע
שנתי (גיבוי מלא)	3	2	כן	פעם בשנה	2 שנים	סופ"ש
חצי-שנתי (גיבוי מלא)	3	2	כן	פעם ברבעון	1 שנה	ינואר, יולי
חודשי (גיבוי מלא)	3	2	כן	פעם ב-4 שבועות	6 חודשים	סופ"ש
שבועי (שינויים מהגיבוי המלא)	3	2	כן	פעם בשבוע	6 חודשים	סופ"ש
יומי (שינויים מהגיבוי האחרון)	2	2	כן	פעם ביום, 5 ימים בשבוע	45 ימים	ימים א-ה
שעתי (שינויים מהגיבוי האחרון)	1	2	כן	פעם בשעה	14 ימים	כל יום
גיבוי מתמשך	1	1	כן	באופן רציף	14 ימים	באופן רציף

טבלה 11: מדיניות בסיסית לדוגמה - גיבוי שרתים פיזיים (Physical Servers)

שרתים וירטואליים:

סוג הגיבוי	מספר העתקים	מספר מדיות	עם עותק מרוחק	תדירות	זמן שמירה	זמן ביצוע
מלא	3	2		פעם אחת בגיבוי הראשון	1 חודש	
אינקרמנטלי	3	2		כל יום	21-28 עותקים אחרונים	לילה
אינקרמנטלי	3	2	כן	כל יום	7 העתקים	מיד עם סיום יום העבודה
מלא סינטטי	3	2	כן	שבועי	2 שבועות	פעם בשבוע
מלא סינטטי	2	2	כן	חודשי	3 חודשים	פעם בחודש
מלא סינטטי	1	2	כן	שנתי	2 שנים	פעם בשנה
גיבוי מתמשך	1	1	כן	באופן רציף	14 ימים	באופן רציף

טבלה 12: מדיניות בסיסית לדוגמה - גיבוי שרתים וירטואליים (Virtual Servers)

8. קיצורי שמות (Acronyms)

פרק מציג את קיצורי השמות בהם נעשה במסמך זה.

שם המונח	ביאור
דוא"ל	דואר אלקטרוני
דו"ח	דין וחשבון
ABAC	Attribute-Based Access Control
ACID	Atomicity, Consistency, Isolation, Durability
ACL	Access Control List
ADC	Application Delivery Controllers
API	Application Programming Interface
BCP	Business Continuity Planning
BMS	Backup Management Server
CIFS	Common Internet File System
CMDB	Configuration Management Database
CRUD	Create, Read, Update, and Delete
DEDUP	De-duplication
DoS	Denial of Service
DR	Disaster Recovery
EAL	Evaluation Assurance Level
EC	Erasure Coding
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
FTPS	FTP Secure / FTP-SSL
GDPR	General Data Protection Regulation
HA	High Availability
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
ICAP	Internet Content Adaptation Protocol
IOC	Indicator of Compromise
IOE	Indicator of Exposure
IP	Internet Protocol
IPS	Intrusion Prevention System

שם המונח	ביאור
KMIP	Management Interoperability Protocol
KMS	Key Management Server
MiTM	Man-in-the-Middle Attack
MS	Media Server
MTBF	Mean Time Between Failures
MTTR	Mean Time to Recovery
NAS	Network Attached Storage
NFS	Network File System
NTFS	New Technology File System
OOB	Out of Band
OSI	Open Systems Interconnection
PaaS	Platform as a Service
PIM	Privileged Identity Management
PLC	Programmable Logic Controller
PS	Physical Server
QoS	Quality of Services
RAdAC	Risk Adaptive-Based Access Control
RAID	Redundant Array of Independent Disks
RAM	Random-Access Memory
RDBMS	Relational Database Management System
REST	Representational State Transfer
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAS	Shared Access Signature
SCM	Secure Configuration Management
SDK	Software Development Kit
SFTP	SSH FTP
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOD	Segregation of Duties
SSH	Secure Shell

שם המונח	ביאור
SSL	Transport Layer Security
TLS	Secure Sockets Layer
TTL	Time to Live
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VM	Virtual Machine
XACML	eXtensible Access Control Markup Language

טבלה 13: 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

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

התמודדות ארגונית במרחב הסייבר עם האיום הפנימי

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

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

מדיניות לאומית להזדהות בטוחה

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

כללי:

על המילה גִּבּוּי

- ✓ https://hebrew-academy.org.il/keyword/%D7%92%D6%BC%D6%B4%D7%91%D6%BC%D7%95%D6%BC%D7%99

גיבוי נתונים - Data backup

- ✓ http://www.yairweissman.com/data-backup-information.html

הבדלים בין Snapshot לגיבוי

- ✓ https://linvirtstor.net/2019/08/25/%D7%94%D7%91%D7%93%D7%9C%D7%99%D7%9D-%D7%91%D7%99%D7%9F-snapshot-%D7%9C%D7%92%D7%99%D7%91%D7%95%D7%99/

נב"ת 355, בנק ישראל

- ✓ https://www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/355.pdf

המשכיות עסקית BCP

- ✓ https://www.methoda.cloud/content/pages/kit_bcp/h_guide-map.asp/#section-2

מרכז החישובים הבינאוניברסיטאי (מחב"א) ומר אייל אסטרין
כיצד לבחור בשירות אחסון מנוהל בענן

- ✓ https://www.iucc.ac.il/he/blog/select-cloud-storage/

מיתוסים בנושא שרידות תשתיות בענן

- ✓ https://www.iucc.ac.il/he/blog/cloud-high-availability-myths/

חקיקה

תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017
חוק הגנת הפרטיות, תשמ"א-1981
תקנות בריאות העם (שמירת רשומות), תשל"ז-1976
חוק חתימה אלקטרונית תשס"א-2001
פקודת מס הכנסה [נוסח חדש]
חוק הארכיונים, תשט"ו-1955
General Data Protection Regulation (GDPR)
PCI Standard

כללי

מקורות מידע באנגלית:

General

AAA Authorization Framework, RFC 2904

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

OWASP API Security

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

Password Storage Cheat Sheet

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

Demystifying Recovery Objectives

- ✓ https://www.veeam.com/blog/rto-rpo-definitions-values-common-practice.html

Alternatives to NDMP [Part 1]

- ✓ https://www.unitrends.com/blog/alternatives-to-ndmp-part-1

Alternatives to NDMP [Part 2]

- ✓ https://www.unitrends.com/blog/alternatives-to-ndmp-part-2

RANSOMWARE GUIDE, CISA

- ✓ https://www.cisa.gov/publication/ransomware-guide

NIST

Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events

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

Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events

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

SP 1800-11a: Executive Summary

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

NIST 800-34 Rev.1 - Contingency Planning Guide for Federal Information Systems

- ✓ https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf

NIST 800-184 - Guide for Cybersecurity Event Recovery

- ✓ https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

***** סוף מסמך *****