



סייבר ישראל
מערך הסייבר הלאומי

דגשים למדיניות גיבוי בעסקים קטנים בראי הגנת הסייבר





דגשים למדיניות גיבוי בעסקים קטנים בראי הגנת הסייבר

יוני 2021

מסמך זה נכתב ע"י מערך הסייבר הלאומי לצורך קידום הגנת הסייבר במשק הישראלי. כל הזכויות שמורות למדינת ישראל - מערך הסייבר הלאומי. המסמך נכתב כשירות לציבור. העתקת המסמך או שילובו במסמכים אחרים כפוף לתנאים הבאים: מתן קרדיט למערך הסייבר הלאומי בפורמט המופיע להלן; שימוש בגרסה העדכנית של המסמך; אי הכנסת שינויים במסמך.

המסמך מכיל מידע מקצועי, אשר יישומו בארגון מצריך היכרות עם מערכות הארגון והתאמה למאפייניו בידי איש מקצוע בתחום הגנת הסייבר.

הערות והתייחסויות למסמך ניתן להעביר למייל: tora@cyber.gov.il



««« דגשים למדיניות גיבוי בעסקים קטנים בראי הגנת הסייבר

1. מבוא

בשנים האחרונות החלה עלייה בתדירות ואיכות תקיפות סייבר אשר מטרתן לפגוע בזמינות ו/או מהימנות המידע המאוחסן בארגון. בכלל זה, ניתן לראות שכיחות גוברת והולכת של תקיפות כופרה (Ransomware) אשר מונעות גישה למידע ע"י הצפנת תוכנו, וזאת בשילוב שיטות שונות אשר מטרתן לפגוע ביכולת הארגון לשחזר מאמצעי הגיבוי והאחסון.

מקובל לראות כי בארגונים גדולים נושא הגיבוי זוכה להתייחסות פרטנית, אך בארגונים קטנים רמת המודעות לנושא זה אינה גבוהה, ולפיכך ארגונים אלו עשויים לגלות ביום פקודה כי הם אינם יכולים לשחזר את המידע במקרה של אירוע סייבר או תקלה.

לאור זאת מומלץ כי עסקים קטנים יאמצו את הדגשים הנסקרים במסמך זה. להרחבה בנושא ראו את המסמך - ["שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור"](#).

2. דגשים למדיניות גיבוי בעסקים קטנים

פרק זה סוקר את הדגשים למדיניות גיבוי בעסקים קטנים:

מס'	הדגש
התנהלות כללית	
1.	מומלץ כי הארגון ימפה באופן עיתי את מיקום נכסי הסייבר והמידע הקיים בארגון. בכלל זה יש לוודא כי המיפוי כולל התייחסות למידע המאוחסן בספק ענן וגורמי צד-שלישי אחרים, ורמת הרגישות/קריטיות של המידע והיקפו.



2. מומלץ כי הארגון יוודא מינוי של בעל תפקיד אשר יהיה אחראי על נושא גיבויים ושחזורים. במקרה של שימוש בשירותי מיקור חוץ מומלץ למנות עובד מהארגון שיהיה אחראי לפיקוח על הספק וביצוע בדיקות תקופות לוודא תקינות הגיבוי.	
3. מומלץ כי הארגון יוודא באופן עיתי כי הוא מימש באופן אפקטיבי את עקרון מתן הרשאות נמוכות (Least Privilege) בחשבונות המשתמשים ושירותי המערכת (Service Accounts) המשרתים את מערכת הגיבוי.	
4. מומלץ כי הארגון יעגן משפטית את דרישות ההגנה על מידע בעת התקשרות מול גורמי צד שלישי, לרבות התייחסות לנושא הגיבוי.	
מדיניות גיבוי	
5. מומלץ כי הארגון יגדיר מדיניות גיבוי לכל פריט מידע לפי רגישות/קריטיות המידע, וזאת תוך התייחסות לרמת הזמינות, המהימנות והשלמות (Integrity) של המידע. ככלל, ככל שהמידע רגיש/קריטי יותר, הארגון עשוי לאמץ מדיניות גיבוי מחמירה יותר. להלן דוגמה לתדירות ביצוע גיבויים בהתאם לסוג הגיבוי: • מספר גיבויים לטובת להתאוששות מהירה, גיבוי מסוג תמונת מצב (Shadow Copy), תמונת צל (Shadow Copy) וכד'. • מספר גיבויים שיש לבצע ביום (גיבוי יומי), גיבוי מלא או גיבוי שינויים בלבד ומספר הדורות לאחר של הגיבוי שיש לשמור (לפי תאריך או לפי מספר גיבויים). • מספר גיבויים שיש לבצע בשבוע (גיבוי שבועי), גיבוי מלא או גיבוי שינויים בלבד ומספר הדורות לאחר של הגיבוי שיש לשמור (לפי תאריך או לפי מספר גיבויים).	



• מספר הגיבויים שיש לבצע בחודש (גיבוי חודשי), גיבוי מלא או גיבוי שינויים בלבד ומספר הדורות לאחר של הגיבוי שיש לשמור (לפי תאריך או לפי מספר גיבויים). • שימוש בגיבוי לארכיון (Archive) לתקופה של מספר שנים. - יצוין כי ככל שמדיניות הגיבוי תהיה מחמירה יותר / "בזבזנית יותר", הארגון עשוי לבחור באסטרטגיה של שילוב בין סוגי גיבוי שונים תוך שמירה על הגיבוי לתקופות שונות. לדוגמה: • גיבוי יומי לשינויים בלבד וזאת תוך שמירה של 7 דורות לכיסוי שבועי. • גיבוי מלא פעם בשבוע, ושמירה 5 דורות לכיסוי חודשי. • גיבוי חודשי מלא (עותק של שבועי הראשון), ושמירה של 12 דורות לכיסוי שנתי.	
6. מומלץ כי הארגון יוודא כי ברשותו מערכת גיבוי בעלת ניהול מרכזי.	
אחסון ושיטת הגיבוי	
7. מומלץ כי הארגון יוודא כי שטחי האחסון לטובת הגיבוי מופרדים משטחי האחסון של מערכות הייצור.	
8. מומלץ כי הארגון יוודא כי ברשותו לפחות שני העתקי גיבוי, כאשר לפחות העתק אחד יאוחסן במתקן מאובטח מחוץ למתחם העבודה, מנותק מהרשת (OFFLINE) במידת האפשר.	
9. מומלץ כי הארגון יוודא כי בעת הצורך הוא משלב סוגי גיבוי שונים הנסמכים על טכנולוגיות שונות. סוגיה זו מהותית לארגונים בעלי מידע קריטי/רגיש בנפחים גדולים.	
10. מומלץ כי הארגון יוודא כי בסיום הגיבוי הוא מנע גישה לקבצי הגיבוי וזאת ע"י הגדרתם לקריאה בלבד (Read Only) או שימוש במדיית אחסון מסוג WORM (Write Once Read Many)	



11.	מומלץ כי הארגון יוודא כי המיקום הלוגי והפיזי לאחסון הגיבוי עומד בדרישות החוק, רגולציה, דרישות חוזיות וצרכים עסקיים.
12.	מומלץ כי הארגון יוודא כי הוא מצפין את הגיבוי. בהינתן כי הגיבוי מאוחסן מחוץ לחצרות הארגון הצפנת עותק הגיבוי הינה קריטית.
13.	מומלץ כי הארגון יוודא כי שיטת הגיבוי אשר יעשה בה שימוש תספק מענה לעמידה במדדים מקובלים (דוגמת משך הזמן הנדרש לשחזור נכס סייבר מאפס או יכולת שחזור גם במקרה של תקלה בגיבוי מקומי). סוגיה זו עשויה להשפיע על הבחירה האם לעשות שימוש בגיבוי מקומי לקלטות, מקומי לדיסק, מקומי למערך גיבוי ייעודי, שירות ענן וכד'.
14.	מומלץ כי הארגון יעשה שימוש בתוכנת גיבוי בעלת מנגנונים מובנים לגילוי, זיהוי וחסיתה של כופרה.
טיפול שוטף	
15.	מומלץ כי הארגון יבצע בדיקות שחזור אחת לתקופה וזאת בהתאם לרגישות/קריטיות המידע, כך שהארגון יוכל להבטיח כי הגיבוי הקיים ברשותו תקין. יש להתייחס בבדיקות לרמת שלמות וזמינות המידע. ככלל, יש לגזור את תדירות ביצוע הבדיקות מרמת הקריטיות או הרגישות של המידע (המחמיר מהשניים). בבדיקות השחזור היזומות מומלץ לבצע שחזור של גיבוי מסוגים שונים, כגון שחזור קובץ בודד, שחזור נכס סייבר שלם קריטי (אחת לשנה לפחות), שחזור תיבת דוא"ל, שחזור בסיס נתונים וכו'. יש לתת את הדעת כי בסיום השחזור יש לבצע בדיקת תקינות, וזאת על-מנת לוודא כי תהליך הגיבוי פועל כמצופה.
16.	מומלץ כי הארגון יוודא אחת לשנה לכל הפחות כי אחראי הגיבוי יבדוק את עדכניות מדיניות הגיבוי, והאם שטחי האחסון המיועדים לגיבוי מוגדרים נכון במדיניות הגיבוי שהוגדרה.



17.	מומלץ כי אחת לתקופה הארגון יוודא את רמת ההגנה על המידע המגובה (ברמה הפיזית והלוגית), וזאת תוך החלת בקורות אבטחה בהתאם למדרג הסיכון. יש לתת את הדעת כי הגיבוי עשוי להכיל את כלל המידע הקיים בארגון, ולפיכך דליפה שלו או פגיעה במהימנותו, שלמותו או בזמינותו עשויה לגרום לנזק מהותי לארגון.
18.	מומלץ כי הארגון יוודא כי בסיום פעולת גיבוי/שחזור תשלח לבעל התפקיד בארגון האחראי על הנושא דו"ח המסכם את תוצאות הפעולה.
19.	מומלץ כי הארגון יוודא כי בטרם ביצוע פעולת הגיבוי/השחזור תתבצע בדיקה מקדימה לגילוי, זיהוי והסרת נזקים (Malwares).
20.	מומלץ כי הארגון יוודא שמירה על עדכניות תוכנה הגיבוי והסוכנים (Agents) המוטמעים בנכסי הסייבר.

***** סוף מסמך *****