חשיבות הגיבוי (Backup) בתשתיות ענן

11/03/2026
כ"ב אדר תשפ"ו

[תקציר]

- ארגונים רבים המשתמשים בתשתיות ענן, עלולים להסתמך על מנגנוני השרידות (Resiliency) והיתירות (Redundancy) המובנים של ספקיות הענן המוכרות (AWS, Azure, Google Cloud) כתחליף לגיבוי נתונים.
- יתירות ושרידות נועדו להבטיח רציפות שירות (Uptime), אך אינן מהוות הגנה מפני אובדן, שיבוש או מחיקת נתונים זדונית, כגון על ידי מתקפת כופרה.

[פרטים]

- גיבוי נדרש כדי להתמודד עם כשל לוגי, טעות אנוש או תקיפה זדונית (לדוגמה, מתקפת כופרה). במקרה של מחיקה שגויה או זדונית של מידע, הצפנת כופרה או פגיעה בבסיס נתונים, מערכות השרידות והיתירות המובנות בענן ישכפלו את הנזק או הפגיעה לכל האתרים בהם פרוסה המערכת. ללא גיבוי עצמאי, ייתכן ולא יתאפשר שחזור מידע זה.

פעולות מידיות לביצוע:

- וודאו כי מוגדרת ומופעלת בתשתית הענן שבשימוש ארגונכם תכנית גיבוי המתאימה לרגישות המידע וחשיבותו לשרידות ארגונכם.
- בצעו באופן עיתי תרגול שחזור מגיבוי באופן שיבטיח הן את תקינות הגיבוי, והן את היכרות המנהלנים את נהלי הגיבוי וכיצד לבצעו במהירות וביעילות.
- התייחסו בתוכנית הגיבוי לאפשרות של גיבוי בענן/אזור שונה מזה שבו פועלת סביבת הייצור שלכם (**ראו סעיף 8 תחת "דרכי התמודדות"**), ליעדי RTO/RPO המתאימים לצרכי הארגון, לשמירה של עותק אחד לפחות באופן שלא יהיה ניתן לשנותו על ידי תוקף או אף בטעות על ידי מנהלן, ולגיבוי הגדרות התשתית (IaC).

שיתוף מידע עם מערך הסייבר הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו.

המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.

[דרכי התמודדות]

מומלץ מאד לוודא כי ההגדרות ונהלי הגיבוי של המידע (כולל גם יישומים ייחודיים של הארגון, קבצי קונפיגורציה, חוקי אבטחה, וכל פרט נוסף הנדרש לשחזור מהיר) הנשמר בסביבת הענן שבשימוש ארגונכם עומדים בהמלצות הבאות:

1. קביעת יעדי RTO (Recovery Time Objective, הזמן המקסימלי שהארגון יכול לאפשר (Acceptable Downtime) עד להתאוששות) ו-RPO (Recovery Point Objective – כמה מידע הארגון יכול להרשות לעצמו שיאבד במקרה של צורך בהתאוששות, נמדד כמשך הזמן מביצוע הגיבוי האחרון עד לאירוע המחייב התאוששות) התואמים את צרכי הארגון ואת הרגולציות החלות עליו.
2. יש לוודא כי לא רק הנתונים מגובים, אלא גם קבצי הגדרות התשתית (IaC - Infrastructure as Code), באמצעות כלים כגון Terraform, CloudFormation, Deployment Manager, Bicep ו- Azure Resource Manager (ARM) Templates. מומלץ לוודא גיבוי מלא ונפרד של קבצי ה-State. ללא גיבוי זה, תהליך הקמת הסביבה מחדש יתארך משמעותית בשל הצורך בהגדרה ידנית של הרשת ומרכיביה השונים.
3. מומלץ מאד להצפין המידע בענן, הן בתנועה והן במנוחה (Transit/Rest), באמצעות אלגוריתמים מוכרים ומומלצים לתכלית זו.
4. הפרדת הרשאות לוגית: אחסון גיבויים בחשבון ענן **נפרד** (Isolated Account) בנוסף לגיבוי בחשבון המוגדר בחשבון הראשי, עם הרשאות גישה **שונות לחלוטין**, **הניתנות אך ורק למנהלנים המורשים לטפל בגיבויים ושחזורים,** ושאינן מוגדרות תחת אותו ארגון (Same Org/Subscription), אלא Tenant נפרד.
5. הגדרת הגיבוי כבלתי ניתן לשינוי (Immutable): הגדרת הגיבויים כמוגנים באמצעות Object Lock או Immutable Storage for Blob Storage, או שימוש ב-(MUA) Multi-user authorization, למניעת מחיקה על ידי תוקפים או טעויות אנוש. יש להגדיר Retention Time למניעת מחיקה בשוגג על ידי מורשה. אם קיים בתשתיות הענן שלכם מנגנון שמאפשר שחזור נתונים גם לאחר מחיקה על ידי תוקף (Soft Delete), מומלץ לבחון השימוש בו.
6. שימוש בכלל הגיבוי 3-2-1-1-0: 3 עותקים (עותק ראשי לשימוש המערכת + 2 עותקים לגיבוי), 2 חשבונות שונים (אחד למערכת הייצור והשני לניהול הגיבוי), גיבוי 1 נשמר מחוץ לסביבה הראשית (ספק ענן שונה/אזור שונה – ראו סעיף 8 להלן), עותק 1 שהוא בלתי ניתן לשינוי (Immutable), ו-0 שגיאות בשחזור עיתי לבדיקת תקינות הגיבוי.
7. ביצוע Snapshot עיתי אינו יכול לשמש כפתרון גיבוי **יחיד**, מאחר ולרוב הוא תלוי באותה תשתית כמו התשתית המקורית, אך כן יכול לסייע בהתאוששות מהירה במקרים מסוימים. גיבוי עמיד כנגד תוקף/כופרה מחייב העברת המידע ל-Vault נפרד או ל-Object Storage ייעודי כדי להבטיח הפרדה לוגית ומניעת מחיקה בשוגג.
8. **בחינת** האפשרות לבצע גיבוי לתשתית ענן שונה (Cross-Cloud) ו/או אזור גיאוגרפי (Region) שונה מזה בו נעשה שימוש בסביבת הייצור (**מומלץ לבחון היבטים <u>משפטיים/פרטיות/רגולציה</u> עבור מקרה זה**), לפחות עבור נתונים קריטיים או מערכות קריטיות.
9. תוקפים שוהים לעיתים זמן רב ברשת הארגונית טרם השבתתה. יש לוודא כי שחזור מהגיבוי מתבצע לסביבה מבודדת, ובדיקת המידע המשוחזר על ידי כלי אבטחה רלוונטיים (AV, Sandbox וכד') לפני החזרתו לסביבת ייצור, כדי לוודא שלא הוכנסו אליו נוזקות או פוגענים רדומים.
10. בדיקת שחזור עיתית באמצעות תרגול של שחזור מלא, אחת לתקופה שתיקבע בנהלי הארגון. מומלץ לבחון האפשרות לבצע תרגול שחזור כבר בתקופה הקרובה, לבדיקת תקינות ההגדרות והיכרות המנהלנים עם הנהלים הרלוונטיים.
11. מומלץ לבחון שימוש במנגנוני היתירות ובשירותי ה-DR הרלוונטיים של ספקיות הענן בנוסף לגיבוי (כגון שימוש ב-Multi-AZ/Multi Region, **ראו סעיף 8 לעיל**). גיבוי ללא יתירות/שרידות יסייע במניעת אובדן מידע, אך השחזור עלול לארוך זמן רב.

12. מומלץ להפעיל ניטור לתהליכי הגיבוי, והתרעה יזומה למנהלנים עבור תקלות באמצעות דוא"ל, SMS, WhatsApp וכד'.

נספח א'

מצ"ב טבלה עם המונחים העיקריים בנושא גיבוי מנוהל עבור 3 סביבות הענן הפופולריות:

מאפיין	**Google Cloud**	**Azure**	**AWS**
שם השירות	**Backup and DR**	**Azure Backup**	**AWS Backup**
היכן נשמרים הגיבויים	Backup Vault / Bucket	Recovery Services Vault	Backup Vault
הגדרת הגיבוי	Backup Snapshot / Image	Recovery Point / Backup Item	Recovery Point
מנגנון הגדרת הגיבוי	Backup Plan	Backup Policy	Backup Plan
ארכיון גיבוי	Archive Storage	Archive Tier / Vault-Archive Tier	S3 Glacier

ניתן להשתמש בנוסף גם בפתרונות הגיבוי הרלוונטיים המובנים בשירותים השונים שבשימושכם.