29/08/2024
כ"ה אב תשפ"ד
סימוכין: 1795

אבטחת גיבויים בענן

תקציר

1. ארגונים רבים וכן משתמשים פרטיים מגבים מידע לסביבת ענן כחלק מאסטרטגיית הגיבוי שלהם.
2. מטרת מסמך זה, הכרת הדרכים העיקריות לאבטח גיבויים אלו מפגיעה או דלף על ידי תוקפים.

פרטים

1. ארגונים ומשתמשים פרטיים כאחד עושים שימוש בגיבוי לענן כחלק מאסטרטגיית הגיבוי שלהם.
2. במסמך מצוינים נושאים שונים הקשורים בגיבוי בכלל ובגיבוי לענן בפרט, אשר יש לתת עליהם את הדעת כאשר משתמשים בגיבוי מסוג זה.

דרכי התמודדות

1. קבעו מדיניות גיבוי ויעדי המשכיות מקובלים דוגמת RTO ו-RPO (יעדי זמן ומידע נדרש לשחזורים).
2. שלבו את מדיניות הגיבוי בתוכניות ההתאוששות מאסון והמשכיות עסקית.
3. וודאו שמדיניות הגיבוי שלכם תואמת את דרישות החוק, הרגולציה, והדרישות החוזיות מול לקוחות, אם קיימות עבור ארגונכם.
4. התאימו את מערכות הגיבוי לסוג המידע המגובה – מערכות קבצים, בסיסי נתונים וכו'.
5. החליטו האם המערכות השונות מחייבות גיבוי מתמשך ורציף או גיבוי עיתי.
6. ככל האפשר, מכנו את תהליכי הגיבוי ובדיקת תקינות הגיבוי כך שיפעלו אוטומטית.
7. הגדירו מדיניות גישה והרשאות מתאימות לגישה למידע המגובה. במערכות ענן יש להתחשב הן בהרשאות המשתמש (IAM), והן במדיניות הגישה המוגדרת למשאב (Access Policy). יש לוודא כי אין סתירה בין הגדרות אלו ואחת אינה מעניקה הרשאות שונות/נוספות מאלו שמוגדרות עבור השניה.

8. מומלץ לוודא כי מערכת הגיבויים בעלת יכולת איתור אנומליה דוגמת שינויים חריגים בנפחי גיבוי, הכללת קבצים בעלי סיומות לא מוכרות, וקבצים בעלי רמת אנטרופיה חריגה.
9. בטרם הוספת המידע לגיבוי, מומלץ לבצע בדיקה לאיתור והסרת פוגענים.
10. אבטחו הגישה לגיבוי באמצעות שימוש באימות רב-גורמי (MFA) ושימוש ב- Conditional Access או יכולת מקבילה אשר ספק הענן מאפשר. העניקו הרשאות בהתאם לעיקרון ה- Least Privilege לכל ישות בעלת גישה לגיבוי או הרשאות ניהול של גיבויים.
11. השתמשו בעיקרון הגיבוי 3-2-1 (3 עותקי מידע לפחות (מקור + 2 עותקים) הנשמרים בשני מקומות שונים ולפחות עותק 1 אינו מקוון בכל רגע נתון.
12. הצפינו המידע בתנועה ובמנוחה.
13. עשו שימוש במגוון אמצעי הגיבוי של תשתיות ספק הענן (Nearline, Offline), והתחשבו בעלות האחסון, לעומת זמינותו, לרבות האפשרות לנייד מידע ישן לתשתית זולה יותר.
14. כחלק מאסטרטגיית הגיבוי, עשו שימוש באמצעי אחסון שאינם ניתנים לשינוי (Immutable) כגון כונני WORM המאפשרים כתיבה פעם אחת ומספר בלתי מוגבל של קריאות. השימוש בארכיון (Archive) עשוי לספק חלופה המאפשרת החלה של מדיניות Data Retention קשיחה.
15. נטרו היטב את מערכות הגיבוי והקפידו לטפל בכל תקלה.
16. בדקו באופן עיתי את תקינות הגדרות הגיבויים (Audit).
17. בחנו שימוש בפתרון CSPM לשם איתור הגדרות תצורה אשר עשויות לחשוף מידע לגורמים לא מורשים. בחנו שימוש בפתרון DSPM לשם איתור מידע ארגוני, סיווגו, ומעקב אחר תנועתו, לצורך טיוב תהליכי הגיבוי.
18. מומלץ לוודא כי המידע המגובה מאוחסן באזורים (Regions) גיאוגרפיים המאושרים בהתאם למדיניות הארגונית, הכוללת התייחסות פרטנית לנושא ריבונות המידע (Data Sovereignty).
19. בדקו באופן עיתי את תקינות הגיבויים ואת היכרותכם עם נהלי השחזור והתאוששות בחירום. עשו שימוש רב ככל האפשר ביכולת Infrastructure as a Code לשחזור המערכות במקרה הצורך.
20. וודאו באופן עיתי כי כל רכיבי מערכות הגיבוי מעודכנים לגרסאות האחרונות.
21. עשו שימוש במערכות אחסון מפתחות של תשתיות הענן דוגמת KMS או HSM לשמירת מפתחות הצפנה וגישה לגיבויים. יש לוודא קיומו של תהליך החלפה עיתי של המפתחות

(Key Rotation), ושמירה מאובטחת של מפתחות פעילים וישנים, לרבות החלת הפרדת סמכויות (SoD) בין המופקדים על השמירה והגישה למפתחות אלו.

22. הפרידו ככל האפשר בין סביבת הייצור לסביבת הגיבוי (יישמו עבור הגיבוי סביבה נפרדת לחלוטין באופן שגם אם תוקף ישיג גישה לרמה העליונה ביותר בסביבת הייצור, הוא לא יוכל לגשת או לפגוע בסביבת הגיבוי). מומלץ כי הגישה לניהול מערכות הגיבוי תהיה ממחשבים ייעודיים המנותקים מסביבת התקשוב הרגילה של המנהלנים.
23. בעת גישה למשאב הקיים בסביבה אחת, מסביבה אחרת, מומלץ לעשות שימוש ב- Private Endpoint (דוגמת Interface endpoints ב-AWS) , כך שהתעבורה תעבור על גבי תשתית ה-Backend של תשתית ספק הענן, ולא על גבי תשתית האינטרנט.
24. אם אתם משתמשים בפתרון Backup as a Service מומלץ לוודא כי ברשות ספק הענן ההסמכה CSA STAR Level 2 (https://cloudsecurityalliance.org/star).

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה בלשהו, 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.