TheMarker IT COMPUTERWORLD it.themarker.com

רמי ניסן 01.10.09 | 14:50

# DRP - כך תגנו על המידע העסקי שלכם במקרה אסון

**אסון מגדלי התאומים הפך את המונח "תוכנית התאוששות מאסון" לבאז-וורד. הנה כמה טיפים שיבטיחו את התאוששות מערך ה-IT בעת הצורך**

בחודש האחרון צוינו שמונה שנים לאסון התאומים. האסון, אשר היווה ציון דרך עולמי בלחימה בטרור, היווה גם ציון דרך בהתייחסות הארגונים בעולם לתחום ההמשכיות העסקית (BCP - Business Continuity Plan) בכלל, ולהתאוששות מאסון של מערכות המידע (DRP - Disaster Recovery Plan), בפרט.

לאחר האסון, המונח DRP, שהיה מוכר עוד קודם לכן, הפך ל- Buzzword. האסון חשף בעוצמה רבה את התלות ההולכת וגוברת במערכות המידע לקיום העסקי התקין של הארגון, וכתוצאה מכך אף את הצורך להגן על מערכות המידע מאירועי טרור, אסונות טבע, נזקים במזיד ותקלות וטעויות אנוש. על פי סקר בנושא התאוששות מאסון אותו פרסמה חברת סימנטק ביוני 2009, כ-60% ממערכות המידע בארגונים הוגדרו כקריטיות.

רבים מבעלי התפקידים הבכירים בארגונים, בדגש על מנהלי מערכות המידע, החלו לעסוק בנושא, בחנו באופן יסודי את מערך הגיבויים שלהם, שיפרו אותו באופן ניכר ואף טרחו ושמרו גיבויים באתר מרוחק. גם כיום, שמונה שנים אחרי האסון, רבים קושרים את המונח DRP עם קיומו של מערך גיבויים תקין בלבד. אכן, ניהול מערך גיבויים תקין הוא תנאי בסיסי והכרחי לתוכנית התאוששות מאסון יעילה ואפקטיבית. עם זאת, מערך גיבויים בלבד, תקין ויעיל ככל שיהיה, אינו מספיק ואינו נותן מענה לכלל המרכיבים הנדרשים להתאוששות אמיתית של מערך ה-IT בעת אסון.

להלן מספר טיפים להכנה של תוכנית התאוששות מאסון, אשר עשויים להבטיח את שרידות מערך ה- IT בעת חירום:

**• הגדירו את הצרכים לחירום**

תהליך זה חייב להתבצע בשיתוף מלא של התחומים העסקיים בארגון, וכחלק מההתארגנות לטיפול בהמשכיות העסקית שלו. האם הארגון זקוק לכל מערכות המידע שלו גם בחירום? כמה זמן ניתן "לחיות" בלי כל אחת מהמערכות? האם יש חלופות לעבודה ללא המערכת (תהליכים ידניים תוך שימוש בטפסים וכדומה)? בחלק מהארגונים קיים גיבוי חם של כל מערך ה- IT לאתר מרוחק. כך, כל הנתונים שהיו ברשות הארגון טרם האסון נשמרו ויהיו זמינים בעת הצורך. אך מהו בדיוק הצורך? לעיתים קווי הנתונים המרוחקים אינם נותנים מענה להפעלת כלל המערכות במקביל. לפיכך יש להיערך למיפוי מערכות ותשתיות קריטיות, תוך ניתוח המשאבים הנדרשים לפעולה בחירום ושל לוחות זמנים.

במהלך התכנון יש להתייחס לגורמים הבאים:

RTO - Recovery Time Objective: בתוך כמה זמן מרגע האסון המערכת צריכה להתחיל ולפעול? מהו זמן ההשבתה שהארגון מוכן לספוג?

RPO - Recovery Point Objective: מהי כמות המידע (לכל מערכת) שהארגון מוכן לאבד? האם הארגון יכול לספוג אובדן נתונים של יום שלם? של מספר שעות? האם איבוד של מידע הוא נסבל? האם עיבוד של מידע הוא נסבל?

**• בדיקת הגיבויים**

לכאורה, רכיב אלמנטרי. עם זאת, בחלק ניכר מהארגונים קיימות לצד מערך גיבויים מסודר ומאורגן קלטות גיבוי שלא נבדקו מעולם. בדיקה תקופתית של הגיבויים באמצעות שחזור נתונים מקלטות הגיבוי, תבטיח למנמ"ר החפץ להישאר בתפקידו, כי בעת חירום ניתן יהיה לסמוך על קלטות הגיבוי והמידע האגור בהן. רצוי שהבדיקה תדגום בכל פעם מערכת אחרת או קבוצה אחרת של קבצים.

**• שמירת הגיבויים באתר מרוחק**

שמירת הגיבויים במשרדי החברה, אפילו בתוך כספת חסינת אש, עלולה שלא לתת מענה הולם להתאוששות במידה ומשרדי הארגון יפגעו באופן קשה, חלילה. הדבר נכון במיוחד כאשר נדרשת יכולת התאוששות מהירה מאתר מרוחק. גם גיבוי חם עלול שלא לתת מענה, כפי שלמדנו מהתקלה שהייתה בבנק הפועלים. לכן, מקובל שעותק של הגיבוי השבועי יישמר הרחק מאתר החברה ויהיה זמין בעת חירום. יש כיום מספר חברות הנותנות את השירות הזה, כולל איסוף והחזרה של הקלטות באופן שוטף.

**• נגישות לקוד מקור**

בשנים האחרונות התעצמה מאד המגמה של התבססות על ספקי תוכנה חיצוניים, אם כחלק מחבילת מדף ואם כפיתוח ייעודי המבוצע במיקור חוץ. מאידך, אנו נמצאים בעיצומו של משבר כלכלי. מה המשמעות של קריסת ספק תוכנה שלכם? מה יהא על קוד המערכת (ובמיוחד על הקוד שפותח במיוחד עבורכם)? כחלק מתוכנית להתאוששות מאסון רצוי להגיע להסכם עם כל אחד מספקי התוכנה המרכזיים של הארגון, שיבטיח את שמירת הקוד בנאמנות בידי צד שלישי. הנאמן יוכל להחליט למסור לכם או לגורם כלשהו המקובל עליכם את קוד המקור של המערכת, ובכך תוכלו להמשיך ולתחזק את מערכות הליבה שלכם (עם קשיים לא מועטים, אמנם).

**• הפעלה מאתר מרוחק**

במידה והארגון מבוסס באופן ניכר על מערכות המידע ואינו יכול לסבול את השבתתן לתקופה ארוכה (ואיזה ארגון כיום מסוגל לזה?), רצוי להגיע להסכם מראש, שיאפשר לכם את הפעלת מערכות המידע המרכזיות מאתר מרוחק. ההסכם יכול להיות עם חברה המתמחה במתן שירותים מעין אלו, עם חברה אחות או אפילו עם חברה מתחרה (תוך גידור הסיכונים הנובעים מצעד שכזה). ההסכם צריך לוודא כי באתר החליפי קיימת תשתית המסוגלת לתת מענה לצרכים המינימאליים שלכם בחירום, כולל הפעלת המערכות הנדרשות, רשת התקשורת, תחנות עבודה עם התוכנות הרלוונטיות וכו'. במקביל להסכם זה צריך להגיע להסכם עם ספק תשתיות התקשורת שלכם, כך שהוא יהיה מסוגל לנתב מחדש את קווי הנתונים והטלפונים שלכם לאתר המרוחק בלוח זמנים סביר.

**• שמירת התוכנית**

במסגרת עבודתנו נחשפנו פעמים רבות לארגונים שטרחו והכינו תוכנית DRP. נחשפנו גם לתוכניות ההתאוששות לטווח הקצר, הכוללות גם מהלך של עבודה ידנית עם טפסים. אולם, בחלק לא קטן מהמקרים התוכנית המפורטת והטפסים המעוצבים היו שמורים - איך לא - במחשב המרכזי. כמובן שבמידה והיה מתרחש אירוע בו היו נזקקים לתוכנית ההתאוששות, היא לא הייתה בנמצא. גם לא תיאור התהליכים הידניים והטפסים המפורטים בתוכנית. מקובל לשמור מספר עותקים מהתוכנית מחוץ לחברה ועל גבי המחשבים הניידים של בעלי התפקידים הבכירים בארגון. כך תהיה התוכנית זמינה ונגישה לבעלי תפקידים במידה ויהיה צורך להפעיל אותה.

**• תרגול, תרגול, תרגול**

על פי הסקר של חברת סימנטק, אחד מכל ארבעה תרגילי התאוששות נכשל. תוכנית התאוששות, טובה ככל שתהיה, לא תפעל כראוי אם לא תורגלה, ואם בעלי התפקידים המופיעים בה אינם מודעים לקיומה ולאופן ההיערכות הנדרשת בחירום. בדיוק כשם שחשוב לבדוק את תקינות הגיבויים, כך הכרחי לתרגל אחת לפרק זמן קצוב את תוכנית ההתאוששות. תרגול מוצלח יחשוף את כל תקלות התכנון של התוכנית, יחשוף ליקויים בהקצאת כ"א להמשך העבודה עם המערכות, בעיות בזמני תגובה של המערכות, ליקויי אבטחת מידע ועוד ועוד. כמובן שצריך לתכנן את התרגול באופן מדוקדק, כך שהמהלך העסקי התקין של הארגון לא ייפגע, אך אין לוותר עליו!

אסון התאומים, כאירוע מכונן, גרם, בין היתר, לעדכונים ניכרים ברגולציה, בתקינה ובסטנדרטים הבינלאומיים המטפלים בתוכניות ההמשכיות העסקית וההתאוששות מאסון. תקנים, הנחיות חדשות ועדכונים מופצים באופן שוטף, הן בחו"ל והן ע"י הרגולטור בארץ. ליווי מקצועי, אשר ישלב מתן מענה הולם לצרכי הארגון, תוך עמידה ברגולציה ובתקנים המקובלים,יכול לסייע לארגון להיערך באופן יעיל, ולהכין תוכניות היערכות.

**הכותב הוא מנהל תחום מערכות מידע בחברת פאהן קנה ניהול בקרה.**