DRP - גיבויים זה לא הכל...

מאת: רמי ניסן, CISA, MBA, מנהל מחלקת ביקורת מערכות מידע

אסון מגדלי התאומים בשנת 2001, אשר היווה ציון דרך עולמי בלחימה בטרור, היווה גם ציון דרך בהתייחסות הארגונים בעולם לתחום ההמשכיות העסקית (Business Continuity Plan - BCP) בכלל, ולהתאוששות מאסון של מערכות המידע (Disaster - DRP Recovery Plan), בפרט.

לאחר האסון, המונח DRP, שהיה מוכר כמובן 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, תקלות וטעויות אנוש. על פי סקר של חברת סימנטק מיוני 2009 בנושא התאוששות מאסון, 60% ממערכות המידע בארגונים שהשתתפו בסקר, הוגדרו כקריטיות.

רבים מבעלי התפקידים הבכירים בארגונים, בדגש על מנהלי מערכות המידע, החלו לעסוק בנושא וכתוצאה מכך בחנו באופן יסודי את מערך הגיבויים שלהם, שיפרו אותו באופן ניכר ואף טרחו ושמרו גיבויים באתר מרוחק.

אופס, האם פספסנו משהו ??

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:

1. 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 וכד')? 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. מהו המינימום? לכן, יש להיערך למיפוי מערכות ותשתיות קריטיות, תוך ניתוח מה צריך לפעול בחירום ובאיזה לוח זמנים. בהקשר לכך, יש לתת את הדעת לשני מושגים מקובלים:

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

Recovery Point Objective - RPO: מהי כמות המידע (לכל מערכת) שהארגון מוכן לאבד. האם הארגון יכול לספוג אובדן נתונים של יום שלם, של מספר שעות, או שאינו מוכן לספוג כל איבוד של מידע.

2. 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, האם שאלתם את עצמכם מה תהיה המשמעות לקריסה של ספק התוכנה שלכם? מה יהא על קוד המערכת (ובמיוחד על הקוד אשר פותח 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 וכך תוכלו להמשיך ולתחזק את מערכות הליבה שלכם (עם קשיים לא מועטים, אמנם).

3. שמירת הגיבויים באתר מרוחק

שמירת הגיבויים במשרדי החברה, אפילו בתוך כספת חסינת אש, עלולה שלא לתת מענה הולם להתאוששות במידה וחלילה משרדי הארגון יפגעו באופן קשה. הדבר נכון במיוחד כאשר נדרשת יכולת התאוששות מהירה, מאתר מרוחק. מאחר ומחיר קווי הנתונים רחבי הפס ירד בשנים האחרונות באופן משמעותי וזמינות הטכנולוגיה למימוש מאידך, רק גדלה והוזלה, הרי שיותר ויותר ארגונים מממשים היום תהליכי גיבוי באופן מקוון. התהליך מבוצע באמצעות שכפול נתונים או תנועות (רפליקציה), השומר על סנכרון בין בסיסי הנתונים המרוחקים. לחילופין, ניתן לממש גיבוי מקוון גם באמצעות גיבוי לאתר אחסון מרוחק המבוצע אחת ליום (בד"כ בשעות הלילה).

במידה ולחברה אין מערך לגיבוי מקוון והגיבויים מבוצעים על גבי קלטות, מקובל שעותק של הגיבוי השבועי יישמר הרחק מאתר החברה, ויהיה זמין בעת חירום.

4. בדיקת הגיבויים

לכאורה, רכיב אלמנטרי. בפועל, בחלק ניכר מהארגונים אותם אנו מלווים, נמצא כי קיים מערך גיבויים מסודר ומאורגן להפליא, אך הגיבויים לא נבדקו מעולם, שלא לדבר על בדיקה תקופתית. בדיקה תקופתית של הגיבויים באמצעות שחזור נתונים מקלטות הגיבוי או מהאתר המרוחק, או באמצעות מעבר לעבודה של ממש מהאתר

 ©2010 Fahn Kanne Control Management Ltd. All rights reserved

המרוחק, תבטיח למנמ"ר החפץ להישאר בתפקידו, כי בעת חירום ניתן יהיה לסמוך על הגיבויים אותם טורח הארגון לבצע באופן שוטף, ועל המידע האגור בהם. רצוי שהבדיקה תדגום בכל פעם מערכת אחרת או קבוצה אחרת של קבצי נתונים.

5. הפעלה מאתר מרוחק

במידה והארגון מבוסס באופן ניכר על מערכות המידע, ואינו יכול לסבול השבתה שלהם 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 (מראש...) להסכם עם ספק תשתיות התקשורת שלכם, כי יהיה מסוגל לנתב מחדש את קווי הנתונים והטלפונים שלכם לאתר המרוחק בלוח זמנים סביר.

6. שמירת התוכנית

במסגרת עבודתנו, נחשפנו פעמים רבות לארגונים אשר טרחו 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... במחשב המרכזי. זה, אשר התוכנית מתיימרת לטפל באופן ההתאוששות מקריסתו. כמובן, שבמידה והיה מתרחש אירוע בו היו נזקקים לתוכנית ההתאוששות, היא לא הייתה בנמצא, כולל גם תיאור התהליכים הידניים והטפסים המפורטים בה. מקובל כי התוכנית תישמר במספר עותקים - הן עותקי נייר (מחוץ לאתר החברה) והן ע"ג המחשבים הניידים של בעלי התפקידים הבכירים בארגון. כך, חלילה במידה ויעלה הצורך להפעיל את התוכנית, היא תהיה זמינה ונגישה לבעלי התפקידים הרלוונטיים.

7. תרגול, תרגול, תרגול...

על פי הסקר של חברת סימנטק, מיוני 2009, **אחד מכל ארבעה תרגילי התאוששות נכשל.** תוכנית התאוששות, טובה ככל שתהיה, לא "תנגן" 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. כמובן שצריך לתכנן את התרגול באופן מדוקדק, כך שהמהלך העסקי התקין של הארגון לא ייפגע, **אך אין לוותר עליו!**

לסיכום

לא עסקנו כאן בהיבטים נוספים של תוכנית ההתאוששות מאסון, כגון: הבטחת עדכניות התוכנית, אמצעי ההגנה על מתקן המחשב ועוד. יש לזכור שגם כאשר מתייחסים רק ל- DRP (ולא לכלל היבטי ההמשכיות העסקית של הארגון), לא ניתן להתעלם מכך שמדובר בתהליך מורכב, הכולל היבטים רבים מעבר לתחום הצר של ה- IT. תהליך זה חייב להתבצע בהנחיה, בתקצוב ובגיבוי מלא של הנהלת הארגון ותוך שיתוף פעולה עם המשתמשים, הן בתכנון ובניית תוכנית ההתאוששות והן בתרגולה.

אסון התאומים כאירוע מכונן, גרם בין היתר גם 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 תוכנית אפקטיבית להתאוששות מאסון.

"אסון התאומים היווה גם ציון דרך בהתייחסות הארגונים בעולם לתחום ההמשכיות העסקית בכלל ולהתאוששות מאסון של מערכות מידע בפרט".

רמי ניסן, CISA, MBA, מנהל מחלקת ביקורת מערכות מידע

 ©2010 Fahn Kanne Control Management Ltd. All rights reserved