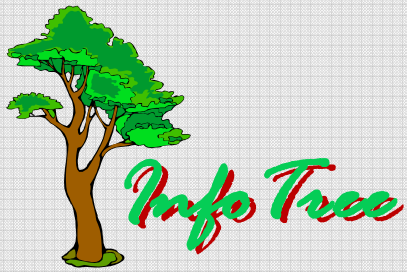

Newsletter #6

לקוח נכבד.

הערכות להתאוששות לפני אסון (DRP) הינו אחד מהנושאים התופסים כותרות בד"כ רק לאחר התרחשות מקרי אסון . נושא זה הינו אחד מהנושאים העיקריים בהערכות הארגון בראיה רחבה ומסודרת במסגרת תחום אבטחת מידע.

במסגרת שירותי חברת סקיוריטרי אנו שמים דגש על נושא של הערכות להתאוששות מפני אסון, במטרה להבטיח כי המידע באתר הלקוח ישמר שלם, אמין ומאובטח במקרה ונגרם לארגון נזק כלשהו במזיד או בשוגג.

בהמשך, מצורף המאמר " המידע הארגוני והמשכיות עסקית " להעשרת הידע בנושא.
לקבלת פרטים נוספים ופניות בנושא, ניתן ליצור עימנו קשר בכתובת
Info@securitree.co.il .

אביאת בר
מהנדסת אבטחת מידע

המידע הארגוני והמשכיות עסקית

מאת: צביקה גורן, יועץ אבטחת מידע בכיר ומרכז נושא DRP

בחברת סקיוריטרי.

אומרים שמודעות הציבור והנכונות להשקיע בהיערכות לאישוש מאסון ובפתרונות שנועדו לאפשר המשכיות עסקית גדלו מאז אירועי 11 בספטמבר 2001 . האומנם ?

אומרים גם שהמלחמה עם עיראק וזיכרונות מלחמת המפרץ שהייתה, תרמו גם הם להכרה בצורך להכנת תוכנית DRP ותכנון להמשכיות הפעילות העסקית (BCP). האומנם ?

עוד אומרים שתלותם הגוברת של גופים וארגונים שונים במידע האגור בתוך מרכזי האחסון ובתוך ה"מחסנים", יצרו תנאים נאותים לתכנון והשקעה בהבטחת שרידותו של המידע. האומנם ?

מה בפועל באמת אירע ?

"המשכיות עסקית" אכן הפכה להיות אחד "הבאזוורדים" החמים (כפי שנכתב באחד מהעיתונים המקצועיים) השגורים בפיהם של אנשי מחשב ומקצוענים, והעניין המקומי והעולמי בנושא גם כן גדל והחלו להישמע בארגונים רבים "קולות" של הכנה לקראת תכנון לאישוש מאסון.

"קולות" - רבים, קולניים ומאותתים על הליכה לקראת תכנון ויישום.

"מעשים" - מועטים, לא מתוכננים, לא מאורגנים ומאופיינים על ידי "רכישות" לא מחושבות.

במרב החברות והארגונים נושא ה"המשכיות העסקית" התמקד ברצון "לשרוד" את המצב הקיים בלא להקדיש שימת לב רבה לתכנון ה"אישוש העסקי" במקרי חירום או אסון.

במקצת מהחברות והארגונים נעשו צעדים מקדמיים המראים נכונות להיכנס לנושא ה"המשכיות העסקית", אך בפועל לא הוחל בתהליכים כלשהם שנועדו למימוש הפרוייקט.

ביתר החברות והארגונים - שמספרם קטן - ננקטו צעדים ראשוניים לקראת תכנון לאישוש עסקי, ורק במספר מזערי של חברות וארגונים נעשו צעדים של ממש בתחום זה.

מה מאפיין את אותם מועטים שהחלו לנקוט בצעדים ממשיים ?

- דאגה ברובד ההנהלה ל"המשכיות פעילותו העסקית של הארגון במקרי חירום או אסון".
- פנייה למערכות המידע של הארגון והצגת דרישה לתכנון והכנה ל"אישוש עסקי" בעת אסון.
- הטלת משימת תכנון ה"המשכיות העסקית" על גורם לא מיומן שנבחר מתוך מערכות מידע.

- התרוצצות לא מתוכננת ובדיקה לא ממוקדת של טכנולוגיות אשר נועדו לאפשר DRP לארגון.
- רכישות לא מחושבות של אמצעים ועזרים - ובפרט מערכי אחסון (Storage) - אשר נועדו לזרז את כניסתו של הארגון לתוך עידן ה-DRP.

כיצד נראים התוצרים הסופיים של אותם מועטים שנקטו צעדים ?

- לארגון קיים אתר מחשוב חלופי (אתר DRP) שלא תמיד נותן את המענה הנדרש בתחום זה.
- הציוד באתר החלופי מהווה שכפול מדויק של הציוד המצוי באתר המחשוב המרכזי של הארגון.
- ניהול המידע באתר החלופי - ובאתר המרכזי - מבוצע באמצעות מערכי אחסון אימתניים.
- המידע המאוחסן באתר החלופי מהווה שכפול "חם" של המידע המאוחסן באתר המרכזי.
- בדרך כלל לא מבוצעים ניסויים (Tests) שמטרתם היא:
  - לבחון את איכות המידע המשוכפל והתאימות שבינו לבין המידע שבאתר המחשוב המרכזי.
  - לבחון את יכולות הארגון לאישוש מערכי המידע במקרי חירום/אסון ושיבה לפעילות שוטפת.
- האתר החלופי ותחזוקתו השוטפת מנוהלים באופן לא מבוקר ובהעדר מדיניות ונהלים כתובים.
- הארגון נעדר תוכנית לגיוס כח-אדם ותכנון לאישוש מערכי המידע בשלבים במקרי חירום/אסון.

מהן המסקנות הנלוות לגבי אותם מועטים שנקטו צעדים ?

- הקמת אתר חלופי איננה מהווה ערובה ליכולות "המשכיות פעילותו העסקית" של הארגון.
- מידע משוכפל ומשודרג באופן "חם" אינו מבטיח אישוש והיחלצות מהירה במקרי חירום/אסון.
- תצורת הפתרון שהותווה יש בה מענה חלקי בלבד לכלל תרחישי החירום או האסון האפשריים.
- הקניית יכולת ל"המשכיות פעילותו העסקית של הארגון" אינה מחייבת השקעות ענק או שימוש באמצעי אחסון, שכפול ושדרוג "חם" של המידע שעלות השקעתם אדירה.

כיצד אם כך מתארגנים ומכינים את התשתית ל"המשכיות עסקית" ?

שלב א' - יזום ו"התנעת" תהליך ההקמה.

- **אפיון המערכות והתהליכים הקריטיים בארגון.**
  - מיפוי המערכות והתהליכים הקריטיים בארגון.
  - דרוג רמת הקריטיות בכל מערכת/תהליך קריטי(ת) שמופו.
  - הערכת פרק זמן מכסימלי לתפקוד הארגון בלעדי המערכת/תהליך.
  - שערוך פרק הזמן הנדרש לשחזור המערכת/תהליך על כל התשתיות המתלוות.
- **מיפוי סיכונים וכשלים במערכות/תהליכים שאופיינו.**
  - מיפוי הסיכונים השונים שיש בהם איום על המערכות/תהליכים הקריטיים בארגון.
  - איתור נקודות הכשל במערכות/תהליכים שמופו הנובעות מהפער שבין הקיים לנדרש.

שלב זה מומלץ ליישם באמצעות דיון בנושא "תרחישי חירום/אסון הרלוונטיים לארגון" תוך כדי הבחנה בין 3 סוגי תרחישים (לפחות):

- אובדן מקומי (Local Lost) - כשל נקודתי בתפקודי מערכת/חומרה/מידע/תשתית.
- אובדן מוחלט (Total Lost) - אובדן מוחלט של כל מערך המחשוב המרכזי באתר המטה.
- אסון ארגוני (Organization Disaster) - אובדן מוחלט של אתר המטה על כל תכולתו.

- **ניתוח הסיכונים שאותרו וקביעת עדיפויות לפתרון.**
  - ניתוח הכשלים/סיכונים שאותרו ודירוגם ביחס לחומרתם מהיבט שרידותו של הארגון.
  - קביעת עדיפויות לטיפול בכשלים/סיכונים שאותרו בהתייחס אל דרגת החומרה שלהם.

שלב ב' - עיצוב פתרון ותכנון מודרג להקמה.

- **איתור חלופה ועיצוב ראשוני של אתר ה-DRP.**
  - בחינת צרכי הארגון והתאמת החלופה העונה על דרישותיו כאתר ה-**DRP**.
  - עיצוב פתרון ראשוני וקביעת המפרט הטכני הנדרש לאישוש מערכי המידע.
- **תכנון מודרג לביצוע פרוייקט ההקמה בשלבים.**
  - תכנון תשתיות השרתים, התקשורת, תחנות העבודה ועזרי מחשוב נלווים.
  - הגדרת משימות, אפיון תפקידים לביצוען והקצאת גבולות אחריות לתפקיד.
  - הכנת **Design Review** והנחת אבני דרך ולו"ז ליישום הפרוייקט בשלבים.
- **פיתוח של** Test Plan **ותכנון עלויות הפרוייקט.**
  - פיתוח תוכנית לביצוע ניסויים (**Tests**) בסיומה של כל אבן דרך שהונחה.
  - תכנון לבדיקת מוכנות הן בהשבתת מערכות מודרגת והן בהשבתה מלאה.
  - תכנון עלויות הפרוייקט המיידיות ותכנון עלויות נוספות לשלבי האישוש המתקדם.

שלב ג' - יישום והטמעת הפתרון בשלבים.

- **הקמת צוותי עבודה וקביעת הספק(ים) לביצוע.**
  - מינוי רכזים, הקמת צוותי עבודה והטלת משימות לביצוע על כל צוות.
  - איתור ספקי חומרה/תוכנה, ביצוע מכרזים, וקביעת הספק(ים) המבצע(ים).
- **ביצוע הפרוייקט בהתאמה לאבני הדרך שהונחו.**
  - הקמת התשתיות באתר החלופי תוך כדי הפרדה בין סביבות העבודה.
  - קביעת תצורת המערכות והטמעת הכלים השונים בהתאם לתכנון שעוצב.
  - יישום מתקדם של הפרוייקט בהיסתמך על אבני הדרך והלו"ז אשר הותוו.
- **פיקוח, בקרה ובחינת תוצרים בכל שלבי הפרוייקט.**
  - ביצוע **Tests** ובחינת התוצרים שהתקבלו בסיומה של כל אבן דרך שהונחה.
  - ניתוח התוצאות, הסקת מסקנות וגיבוש תהליכי עבודה לכל אבן דרך שהסתיימה.
  - ביצוע בדיקות מוכנות בסיום הפרוייקט תוך כדי הדמיית השבתות של מערכים שונים.

שלב ד' – תחזוקה, פיקוח, בקרה וענון תקופתי.

- **תכנון לתפעול אתר המחשוב החלופי בעתות חירום/אסון.**
  - קביעת מדיניות ארגונית לאישוש ולהמשכיות עסקית במקרי חירום/אסון.
  - תכנון לאישוש ראשוני ולאישוש מתקדם בשלבים בהתאם להגדרות הארגון.
  - הגדרת צוותים ותפקידים לביצוע משימות אישוש ותחימת גבולות האחריות.
  - תכנון לפינוי אתר(י) הארגון במקרי אסון ולגיוס כ"א וציוותו לפי תפקידי אישוש.
  - תכנון לטיפול בלקוחות/ספקים/סניפים של הארגון בזמן המעבר עד לאישוש מלא.
  - הכנת תיק נהלים לגיוס אנוש, תפעולו, ומהלכי אישוש מערכי המידע במקרי אסון.
- **תכנון לתחזוקה שוטפת של אתר המחשוב החלופי.**
  - קביעת מדיניות ארגונית לתחזוקתו השוטפת של אתר המחשוב החלופי.
  - הקצאת כח-אדם והכנת תוכנית מפורטת לאופן תחזוקתו של האתר החלופי.
  - הכנת נהלים לתחזוקת האתר החלופי וביצוע הדמיית תרגילי DRP/BCP תקופתיים.
- **תכנון לפיקוח, בקרה וביצוע רענונים תקופתיים.**
  - התאמת שינויי תצורה תקופתיים בתשתיות המחשוב וכח האדם שבאתר החלופי.
  - ביצוע Tests לשינויים בתצורת מערכי המחשוב ותכנון בקרות תקופתיות שוטפות.
  - עדכון תוכניות ה-DR ונהלי האישוש בארגון בעקבות שינויים וביצוע רענונים תקופתיים.

לסיכום ניתן לומר, "המשכיות עסקית" בארגון איננה שכפול של מערך המחשוב המרכזי וגם לא השקעות עתק בתשתיות אחסון ומערכי ניהול נתונים. תכנון לאישוש ולהמשכיות עסקית דורשים הבנת צרכי הארגון, "ראייה" מרחבית וכוללת של אסטרטגיית האישוש, ויכולות ניתוח והתאמת פתרון אופטימלי הנותן מענה מירבי לדרישות הארגון ולהמשכיותו העסקית גם בעתות אסון.

ולכל אלה הסבורים שביכולתם להקים בעצמם את הפרוייקט הנ"ל – וללא סיוע של "מקצוענים" – אני מאחל "בהצלחה".