

"הדרישות לגיבוי
הסביבה הווירטואלית
שונות מאלה הקיימות
המוכרות בעולם הפיזי.
הווירטואליזציה מביאה
הזדמנויות חדשות
ומעמידה אתגרים
חדשים בעולם ההגנה
על המידע וגיבוי"



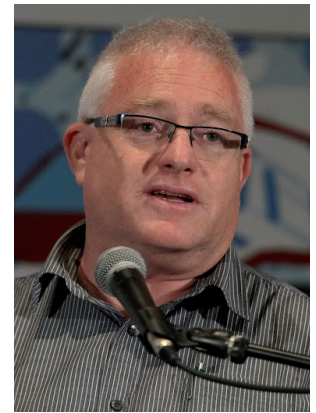
אמיר מרואני

מרואני אמר, כי החברה פעילה הן בסביבה הווירטואלית של VMware והן בזו של מיקרוסופט. לדבריו, "מטרתנו היא לשכלל את מהירות הגיבוי, לצמצם את משך חלון הגיבוי כך שהגיבוי לא יהיה נטל על מנהלי התשתיות הארגוניים". הוא סיים בציין, כי "הכלים שלנו מספקים התאוששות מהירה, גמישה ואמינה של יישומים ונתונים וירטואליים. אנחנו משלבים גיבוי ושכפול בפתרון יחיד, וממציאים מחדש את הגנת הנתונים עבור סביבות וירטואליות".

למגוון היבטים - החל מטיפול בפניו האשפה, עבור בטיפול במוגבלים מוחית ופיזית וכלה במתקני קירור לאחסון גופות לאחר אסון. לא תעזור שום תוכנית DRP אם לבכירי העירייה לא תהיה יכולת לתקשר בטלפון או במכשירי קשר".

"הגיבוי בסביבה הווירטואלית הופך למיינסטרים"

"הגיבוי בסביבה הווירטואלית הופך למיינסטרים ויש לו צרכים שונים מהגיבוי בעולם הפיזי, שאליו היו ארגונים רגילים", כך



שמוליק לשקו

אמר אמיר מרואני, מנהל קדם מכירות ב-Veeam ישראל. לדבריו, "הדרישות לגיבוי הסביבה הווירטואלית שונות מאלה הקיימות והמוכרות בעולם הפיזי. הווירטואליזציה מביאה הזדמנויות חדשות ומעמידה אתגרים חדשים בעולם ההגנה על המידע וגיבוי". הוא ציין, כי "ייחודה של Veeam הוא בכך שהיא נולדה בעולם הגיבוי לסביבות וירטואליות ובשל כך, זו התמחותה. בניגוד לכלים שנועדו לגיבוי בעולם הפיזי אנחנו מתכוונים לגיבוי ולהגנה בעולם הווירטואלי. יש לכך משמעויות נוספות - בהיבטים הטכנולוגיים ובהיבטי העלויות".

מה שלא מתורגל, לא עובד

ראייה של מכלול האיומים שעומדים מולנו - הן ברמה האזרחית והן ברמה הלאומית - מלמדת שאם באמת אנו רוצים להיות ערוכים כהלכה לכל תרחיש, ביטחוני או אזרחי, עלינו להקצות לנושא ה-DRP את המשאבים הנכונים ♦ מילת המפתח היא תרגול, תרגול ועוד פעם תרגול

תרגול ועוד פעם תרגול. זה נשמע כמו סיסמה צבאית, שאפילו מפקד ממר"ם - אל"מ חנוך א', ציין בדבריו: מה שלא עובד בשגרה, לא יעבוד בחירום. או במילים אחרות: מה שלא מתורגל לפחות פעמיים או שלוש בשנה, סביר שלא ייתן את המענה בשעת חירום.

התרגול, כידוע, הוא הנקודה החלשה של רוב הארגונים. בשנתיים האחרונות מרבים לדבר עליו, אבל ממעטים לעשות אותו. בכנס הבוקר הובאו דוגמאות לתרגולים של מערכות גיבוי ו-DRP שונות. נכון שזה עניין של תקציב, אבל ראייה של מכלול האיומים שעומדים מולנו - הן ברמה האזרחית והן ברמה הלאומית - מלמדת שאם באמת אנו רוצים להיות ערוכים כהלכה לכל תרחיש, ביטחוני או אזרחי, חייבים להקצות לנושא את המשאבים הנכונים.

בכנס הוצגו, כמוכן, גם כל הפתרונות שמציעות החברות הטכנולוגיות שפועלות בשוק הזה. שוב ושוב הוכח, כי הכלים והאמצעים קיימים - ולא מהיום. האתגר המרכזי הוא הגברת המודעות והיישום הנכון של כלים אלו, כדי שנהיה מוכנים לכל צרה.

יהודה קונפורטס

אחרים, כמו שריפות, קריסות מבנים, תקלות בתשתיות תחבורה, שיבושים באספקת מים וחשמל, תשתיות תקשורת שקורסות ועוד ועוד. ועוד. חלק מאותם האיומים כבר התממשו, לצערנו, בשנים האחרונות וסביר להניח שנאלץ להתמודד עמם שוב בעתיד.

בין הדוברים השונים בכנס היו גם נציגים של מגזרים בולטים במשק, כמו למשל המגזר הפיננסי, אותו ייצג **חזי כאלו** - מנכ"ל בנק ישראל, המגזר המוניציפלי, שיוצג על ידי **רון שלום** - מנמ"ר עיריית פתח תקווה, מגזר הבריאות, באמצעות **דורון יצחקי** משירותי בריאות כללית ועוד. כל אחד מהמגזרים הללו נערך בדרכו שלו לתרחישי אסון. כל אחד מהם יודע שלא מספיק לקיים מדיניות לאומית כללית להיערכות והמשכיות עסקית, אלא צריך לרדת לפרטים הקטנים בכל תחום ומגזר. הרי המשמעות של המשכיות עסקית היא התאוששות מפגיעה בתשתיות ובמערכות מתחת לרדאר. הכוונה היא לאותן נקודות רגישות שללא תכנון נכון והערכות רציפה, עלולות להיות הנקודות החשופות והרגישות ביותר.

וכאן מגיע המסר המרכזי של הכנס: תרגול,

כנס DRP לאומי התקיים ימים בודדים לאחר תרגיל החירום הלאומי שנערך באחרונה. החלק הפומבי שלו התמקד בתרגול האזרחים בירידה למקלטים ובמצאית מרחבים מוגנים במקדה של הפגזות טילים. על פי נתונים ראשוניים של המשרד להגנת העורף, החלק הזה של התרגיל עבר יחסית בשלום. לא כולם רצו לממ"דים, אבל המודעות היתה ניכרת.

אך אחרי שהעורף יצא בשלום מהמקלטים, עליו להמשיך ולקיים חיי שיגרה. זה אומר שעליו להיות מסוגל להמשיך ולהפעיל את המערכות הקריטיות, שבלעדן אי אפשר לספק שירותים ברמה העסקית, העירונית והלאומית. הנקודה הזו היוותה את אחד המסרים שליוו את כנס DRP לאומי לאורך כל הדרך. למרות שקיימת לכאורה הפרדה בין DRP אזרחי לצבאי, בסופו של דבר מדובר באותה מדינה ובאותם אנשים.

מסר נוסף שעבר בכנס הוא, שבניגוד למה שנהוג לחשוב באחרונה, ההיערכות להמשכיות עסקית (BCP) אינה רק פועל יוצא של איום הסייבר. אמנם מדובר באיום ממש, שיכול בהחלט לשבש מערכות - אבל לא רק. במציאות הישראלית קיימים איומים רבים