

לדברי פרנק, "יש לבנות נכון מערך מיחשוב מגובה ושריד, משמע לטפל בכלל ההיבטים: גיבוי, שרידות, ביצועים ועומסים, אבטחת מידע, אבטחת איכות של תהליכים, מערכות ונתונים". "בנוסף", ציין, "יש לתרגל את המעבר לאתר הגיבוי, על מנת לוודא שבעת חירום, הוא יבוצע בצורה חלקה. התרגול צריך להיות מבוצע בשלבים: תרגילים קטנים לרכיבים בודדים ומערכות; תרגיל מלא עם אתר ראשי 'חי'; ותרגיל מלא עם אתר ראשי 'מת', משמע - ניתוק התקשורת על מנת לוודא את המוכנות לדילוג של הדטה סנטר, על לבצע מעבר הדרגתי רב-שלבי, על בסיס תוכנית מפורטת, שנבנתה על פי ניסיון מוכח ולקחים מהתרגילים שנערכו קודם לכן".



אלי פרנק

הוא הוסיף, כי "בהיבט הגיבוי והשרידות, יש לנקוט שלושה צעדים: הראשון הוא בניית מערך גיבוי ושרידות, תוך התייחסות לרמת הרכיב הבודד, המערכת הבודדת וברמת האתר (DRP). הצעד השני הוא וירטואליזציה, שהיא בעלת תרומה משמעותית ביותר לשיפור הגיבוי, השרידות והזמינות, בכך שהיא מאפשרת דילוג בין אתרים, ללא השבתה ותוך שמירה על רציפות השרות

והמשכיות עסקית. לאחר מכן יש את הצעד השלישי, שהוא הקריטי ביותר - התרגול. חייבים לתרגל מצבים של השבתות ואסונות כדי להבטיח שביום פקודה, כשמתרחש אסון והדטה סנטר באתר הראשי יוצא מכלל פעילות, יבוצע הדילוג כמו שצריך והארגון יוכל להמשיך לפעול תוך הבטחות על אתר ה-DR".

פרנק ציין, כי בתפקידו הקודם, כמנמ"ר בוק, הוא היה אחראי לבניית הדטה סנטר החדש של החברה, וזה היווה בסיס לפרויקט DRP שהתקיים בה. "הפרויקט הזה מנטרל את אחד הסיכונים הגדולים ביותר שעומדים בפני כל חברה מודרנית כיום - נפילת אתר המיחשוב", ציין. "במסגרת הפרויקט יצרנו מערכת DR של כלל מערך המיחשוב בחברה, ללא יוצא מן הכלל. ביצענו תרגול ייחודי של פעילות החברה, למשך יום עבודה מלא מאתר הגיבוי. פיתחנו מתודולוגיה ייחודית ויעילה לשליטה במערך הפעילות המורכב לתרגיל ותחזוקה למצב אמת. כמו כן, במסגרת התרגיל דימינו מצב של אסון מלא במתקן הראשי שלנו וכל הפעילות הועברה לאתר המשני, של הגיבוי. בדרך זו יצרנו BCP אמיתי, לכלל חטיבת ה-IT ולחברה כולה".

"להסיט את המבט החוצה כדי לגלות את איומי הסייבר"

"למרות הדמיון והחפיפה החלקית ביניהם, הסייבר ואבטחת המידע אינם זהים. בשל התגברות הופעתם של איומי הסייבר, על מנהלי אבטחת המידע בארגונים להסיט את המבט שלהם מבפנים החוצה, לעבר האיומים המצויים מחוץ לארגון", כך אמר **אופיר זילביגר**, מנכ"ל SECOZ. בדבריו הגדיר זילביגר מהו סייבר. "ההגדרה של סייבר היא מרחב דיגיטלי הכולל מערכות מידע, תקשורת מחשבים פנימית וחיצונית, תקשורת טלפונית, תקשורת סלולר, אמצעים ניידים, תשתיות פיזיות מבוקרות מחשב והגורם האנושי". הוא אמר, כי "בעבר, כדי להיערך מפני מתקפות סייבר, מנהלי אבטחת המידע היו עוסקים בהתבוננות פנימה, לתוך הארגון, בבחינת 'להגן על המבצר'. בימים אלה, לאחר הופעת איומי הסייבר, עליהם להיות ערוכים בשני כיוונים - פנים וחץ. במסגרת ההתבוננות החוצה, עליהם לייצר ולצרוך מודיעין איכותי על הקורה בחוץ: מה מתכננים ה-'רעים', מה הם יודעים, מה הם מפרסמים ברשתות החברתיות ומה נכתב בצד האפל של האינטרנט".

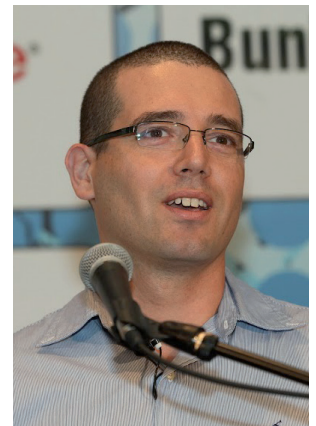
"תחומי אבטחת המידע והסייבר משיקים וחופפים במידה רבה, אולם הם אינם זהים", הוסיף. הוא דימה את שכבת הסייבר כאחת מעל לזו

DR הוא משאבת כסף מטורפת בעוד שהענף מספק מענה עם עלויות נמוכות", אמר פז. הוא סיים בציינו, כי סינגולר מספקת מערכת המשכפלת את תשתיות המידע ומאפשרת לשעתק מתשתית אחת לכל תשתית אחרת. "אנו מציעים פתרונות DRP בענן, על פי דרישה, כך שהארגון משלם לפי שימוש ולא רוכש דטה-סנטר גדול ויקר".

"מה שלא יעבוד בשוטף לא יעבוד בחירום"

"המניע למימוש ולבניית פתרון גיבוי בתצורת Active-Active בין האתר הראשי לאתר הגיבוי בארגונים הוא ההבנה לפיה מה שלא יעבוד בשוטף לא יעבוד בחירום", כך אמר **דורון יצחקי**, מנהל משאבי תשתיות ושרות באגף המיחשוב של שירותי בריאות כללית.

בדבריו תיאר יצחקי את שלבי התפתחות פתרונות המשכיות העסקית



ארז פז



דורון יצחקי

בארגונים בכלל ובכללית בפרט: גיבוי נתונים יציבים בתוך המתקן, בניית מנגנוני שרידות פנים מתקנית, גיבוי חם על בסיס שכפול מידע לאתר חיצוני, זמינות של משאבי המיחשוב במתקן הגיבוי ופעילות מלאה, באופן שוטף, של שני המתקנים.

הוא פירט את הנימוקים למימוש פתרון גיבוי בתצורת Active-Active: "מימוש פתרון שכזה לכל הרכיבים מאפשר שמירה על כשירות אתר ה-DRP ברמה היומיומית. סיבות נוספות הן שזמן הדילוג לאתר הגיבוי מהיר יותר, ניתן לבצע בדרך זו תרגול של מוכנות אתר ה-DR, תוך פגיעה מינימלית בזמינות אתר

האם, יש ניצול מיטבי של משאבי אתר ה-DR ביומים השוטף ומגנן, באתר פסיבי, גם אם הדילוג נעשה באופן מוצלח, התצורה לא תהיה רלוונטית ועדכנית".

יצחקי פרס בפני משתתפי הכנס את שלבי המימוש של תוכנית ההתאוששות מאסון בשירותי בריאות כללית: מיפוי תהליכים קריטיים והערכת סיכונים; קביעת מערכות אסטרטגיות להפעלה ב-DRP; הקמת מתקן גיבוי וחיבורו בתקשורת רחבת פס לאתר האם; מימוש גיבוי חם של המידע; בניית משאבי מיחשוב באתר הגיבוי למערכות האסטרטגיות; ביצוע בדיקה של מוכנות טכנית; חיבור התקשורת של אתרי הקצה לשני המתקנים במקביל; הכנת נהלים וביצוע תרגילי דילוגים למשך יותר מיממה; והפקת לקחים ותיקון.

לסיום, ציטט יצחקי פסוקים מפרק ל"ב בספר בראשית, בו מסופר על יעקב אבינו, שחשש מפגיעת אחיו, עשו, ועשה גיבוי: "ויירא יעקב מאד מעשו... ויחץ את העם אשר אתו לשני מחנות ויאמר: אם יבוא עשו אל המחנה האחת והיכהו, והיה המחנה הנשאר לפליטה".

"לבנות נכון את מערך המיחשוב"

"יש לבנות באופן הנכון מערך מיחשוב מגובה ושריד, על מנת להבטיח המשכיות עסקית ורציפות תפקודית של הארגון", כך אמר **אלי פרנק**, מנכ"ל FrankIT.