

מעולה בחלק מהמקרים", אמר. דולב ציין, כי "אסור לחכות להנחיה או לרגולציה. קיים ידע רב בנושא. כל חברה, רשות מקומית או משרד ממשלתי נדרשים לבצע חשיבה והיערכות לנושא ההמשכיות העסקית". עוד הוא אמר, כי הוא מודע לכך ש-"פתרונות בתחום עולים כסף, אולם ניתן לערוך השקעה הדרגתית בנושא שסופה היערכות להתאוששות מאסון (DRP)".

"גם על המדינה לבצע היערכות מחשבתית בנושא", סיכם דולב. "אנחנו חייבים לקחת את הידע שיש לנו בתחום, לשתף אותו ולהיערך לקראתו. צריך לעשות זאת כבר כיום".

### "חשיבות לרציפות התפקודית בהיבט הגעת המידע לשטח"

"יש חשיבות לסוגיית הרציפות התפקודית בהיבט של הגעת המידע לשטח - בחירום ובשגרה", כך אמר אל"מ (מיל) **יוני גדג**, מנכ"ל איחוד הצלה.

לדברי גדג, איחוד הצלה הוא ארגון כונני רפואת חירום שמונה 2,000 מתנדבים. הוא ציין ש-"מטרת העל שלנו היא להגיע ראשונים לאירוע חירום. הפעילות שלנו משלימה את זו של מגן דוד אדום. ממוצע ההגעה שלנו עומד על ארבע דקות, בעוד שאנשי מגן דוד אדום מגיעים אחרי 13-15 דקות". עוד הוא אמר, כי הארגון עורך שיתופי פעולה עם מכבי האש ועם ארגוני חילוץ.

איחוד הצלה, הוסיף, הוקם לפני כ-20 שנה על ידי קבוצת אזרחים שהחליטו ללמוד קורס עזרה ראשונה, במטרה לטפל בהתנדבות, עד להגעת אמבולנס. במקרי חירום רפואיים המתרחשים באזור מגוריהם. חברי הקבוצה עברו הכשרות מתאימות והחלו לפעול ברחבי הארץ. עם

השנים התרחב, התפתח והתמסד הארגון. גדג ציין, כי הארגון הוא איחוד של ארגוני הצלה מקומיים, שהתאגדו בשנים האחרונות לאיגוד גג אחד.

הוא הוסיף שהחובשים של הארגון מטפלים בפגיעות ובפציעות שונות המתרחשות בשגרה



יוני גדג'

בכל עת בכל מקום בארץ - למשל התקפי לב, תאונות דרכים, חולים וקשישים שנקלעו למצוקה, תינוקות שנחנקו, ועד פיגועי טרור קשים. לדבריו, "במקרי חירום רפואיים, הרגעים הראשונים הם הקריטיים ביותר לצורך ייצוב מצבו של החולה או הפצוע. ככל שחובש יגיע מהר יותר להעניק את הטיפול הראשוני, עם ציוד רפואי מתקדם, כך יגברו סיכויי החולה או הפצוע להחלים ולהימנע מנזק בלתי הפיך".

### "לא כל גוף צריך BCP"

"על המדינה לסווג את הגופים העסקיים השונים שבתחומה ולהגדיר 'תקינה', משמע - מהן הדרישות העקרוניות שצריך כל גוף שכזה. בסופו של התהליך יוברר, כי לא כל גוף צריך BCP", כך אמר **גונן ורדי**, סמנכ"ל בונקרסק.

לדברי ורדי, "זהו אבסורד שהמדינה לא הנפיקה עד היום חוזר ובו הנחיות מפורטות, המנחה את חברות הסלולר כיצד עליהן לפעול ואיך עליהן להיערך. נדרש לתת הנחיות מי צריך BCP וכיצד".

הוא ציין כמה פרויקטים שביצעה החברה בקרב לקוחות ארגוניים שונים. "פרופ' **סטנלי פישר**, נגיד בנק ישראל, הבין שנפילה של מערכות ה-IT של הבנק היא בעלת השלכות חמורות הרבה מעבר לכך שהן

והביטחוניים, בעלי מידע רגיש ביותר, המופקדים על הנושא בשעת חירום". הוא ציין, כי "יש פער וחוסר יחס ברמת ההשקעה בהגנה קיברנטית בין הזרועות האזרחיים לאלה הביטחוניים".



אמיר גרובייס

ניתן לזהות בעולם ובישראל, אמר גרובייס, "כי הרגולטורים השונים מסייעים במידה לא מעטה לשינוי ברמת המודעות ולהשקעה הקיימת בקרב הלקוחות המונחים בתחום הסייבר. חלק מהלקוחות האמורים להיות משולבים בפרויקט, אינם נמצאים תחת הנחיות כלשהן ונעדרים קווים מנחים, העשויים לשנות את המצב הבעייתי הנתון בישראל".

לדבריו, "מרכזי שליטה ואתרי גיבוי ובקרה נוספים בשעת חירום מקבלים נתונים מאתרים רבים ומגוונים. אולם, מרכזים אלו הופכים לנקודת חולשה קיברנטית, כי תקיפות יכולות לעבור דרכן מאתר אחד לשני".

הפיירווול, אמר גרובייס, "המהווה טכנולוגיה פופולרית לחיבור רשתות, חוגג 40 שנות קיום, ורוב ההאקרים כבר יודעים לעקוף אותו מזמן. במערכות צבאיות, בדומה לתשתיות קריטיות, ישנה חשיבות ניכרת לזמינות המידע, ולכן האתגר הראשי הוא לאפשר זמינות של המידע, מבלי לחשוף מערכות רגישות ביטחוניות לאיומי סייבר חיצוניים".

הוא סיכם בציינו, כי פתרונות אבטחת הרשתות של החברה "מאפשרים חיבור בין רשתות בעלות רגישות שונה באופן חד כיווני ומאובטח, תוך תמיכה בצרכים העסקיים של הארגון, ומבלי לחשוף את הרשתות הללו לאיומים של מתקפות סייבר, סייבר-טרור והאקינג מרשתות חיצוניות. כך, ניתן לשלב בין הצורך לזמינות המידע בזמן אמת לבין אבטחה מרבית מפני פריצות. החברה מפתחת טכנולוגיות ומוצרים לאבטחת מידע ורשתות בסביבות תעשייתיות וביטחוניות, ומוצריה מספקים מגוון רב של פתרונות עבור תשתיות קריטיות, חברות תעשייתיות, וכן גופי ביטחון. הפתרונות שלנו מסייעים לתשתיות ולתשתיות חיוניות לעמוד בדרישות של מגוון סטנדרטים ורגולציות בינלאומיים בתחום אבטחת סייבר".

### "ה-BCP הופך לחיוני כי קשה להגן בסייבר"

"הנחת היסוד היא שבשנים הקרובות, מערכות תפעוליות מבוססות מחשב ישותקו בשל מתקפות סייבר, מבלי שיחזרו לפעול בתוך זמן קצר, אם בכלל. יהיה קשה עד בלתי אפשרי להגן מפני מתקפות סייבר. בשל כך, התוכנית להמשכיות עסקית (BCP) מקבלת משנה חשיבות", כך אמר **בוני דולב**, מנכ"ל



בוני דולב

ClearSky.

לדברי דולב, לשעבר מנהל ממשל זמין, "על מנת להתגונן מפני מתקפות סייבר נדרשים פתרונות יצירתיים, ואין לבחול בפתרונות בסגנון הדפסות נתונים על גבי נייר, גיבויים בחו"ל, חלוקת טלפונים ניידים על פני כמה ספקיות

סלולר ועוד. אסור להשאיר את החשיבה והפתרונות לאנשי ה-IT בלבד. כך, למשל, "הרעיון של הקמת מערך מיחשוב חלופי מבוסס ענן הוא רעיון