

מודעים לכך שאנו במידה רבה מאחרים את הרכבת, אותה רכבת לנגב שמסילתה תהיה סלולה אולי בעוד כמה שנים. הקמת קריית הסייבר עצמה לא מספיקה: הממשלה, על זרועותיה השונות, חייבת להקדיש מחשבה עמוקה כיצד מאכלסים אותה עם צעירים שרואים במקצוע הסייבר עתיד מקצוע שאפשר להתפתח בו.

כדאי להקשיב לאזהרותיו החוזרות ונשנות של אחד מאנשי המקצוע הוותיקים בענף, אבי וייסמן, שחוזר ומתריע מעל כל במה אפשרית, כי בניגוד מוחלט לתדמיתה, ישראל מפגרת מאוד בכל הקשור למגננה מפני הסייבר. זה נכון בעיקר במגזר האזרחי, ולא רק בגלל מחסור בכוח אדם, אלא בשל העדר מדיניות ברורה של הרגולטור. זה צריך לחייב את המגזר העסקי להיערך מפני מתקפות סייבר, שתבואנה מכל סיבה שהיא.

השורה התחתונה: התרומה של EMC להקמת קריית הסייבר בדרום היא חשובה, מכמה טעמים. היא חשובה למאמץ הלאומי, לעצם הקמתה באזור הדרום, שצפוי בשנים הקרובות לקבל תנופה אדירה, בין היתר בשל מעבר צה"ל לנגב. אולם אסור לחשוב לרגע שבכך הסתיימו המאמצים בטיפול בסוגיה זו. על הממשלה להתגייס, יחד עם התעשייה, כדי להחדיר את המודעות לפעילות הסייבר בקרב כל שכבות האוכלוסייה בישראל. זאת, כדי שהקריה החשובה שעומדת לקום לא תהפוך לעוד פיל לבן.

התוות את הדרך שבה ישראל צריכה להתמודד עם איומי הסייבר, במישור האזרחי ולא דווקא הצבאי. אחד החסמים המרכזיים שגרם לכך שאנו צועדים בצעדי צב למימוש הפוטנציאל שלנו בתחום לוחמת הסייבר, הוא הגורם האנושי. בישראל אין מספיק אנשים בעלי ידע והכשרה ללוחמת הסייבר. "יחידות ה-8200 למיניהן בחילות השונים עדיין לא הצליחו לייצר את הקאדר האמיתי שיביא לפריצת דרך. המציאות הזו לא נולדה אתמול: היא תולדה של הזנחה רבת שנים, שבהן ממשלות ישראל לדורותיהן, וגם התעשייה במידה רבה, לא דאגו להכשיר מסלולי לימוד והסבת צעירים לתחומים אלו. השנים האלו היו קריטיות, שבהן השד הגרעיני האיראני התפתח לו בשקט, הרחק מעין הזרקורים, עד שהגיע למימדים עצומים וכמעט לנקודת האל-חזור.

המאבק בגרעין האיראני אינו חד מימדי. אבל למאבק הזה יש מימדים טכנולוגיים מאחורי הקלעים. המאבק אינו רק על משלוח טיל זה או אחר, אלא על יכולת של מדינות, גורמים עוינים, ארגוני טרור ואחרים - שיכולים לגרום נזק כבד למדינות אחרות, לא פחות מאשר אותו גרעין עלום ומאיים. לכן, יש הסבורים כי אין מנוס מלקשור את הגרעין האיראני עם סייבר, לצד העובדה כי הסייבר הוא איום בפני עצמו, כזה שצריך להיערך אליו. כל מקבלי ההחלטות בישראל, בדרג האזרחי והצבאי, צריכים להיות

## גיבוי חירום - לא על חשבון ההמשכיות העסקית

ככל שמתגבר הטרור הקיברנטי מצטמצם הדיון הרחב על היערכות למקרי אסון לתחום ה-DR - והתוכניות להמשכיות עסקית, שחשובות לארגון לא פחות, סובלות מכך • המנמ"רים יודעים את זה - אז למה חלק גדול מהם לא עושים מספיק?

לשגרה בזמן קצר ככל הניתן ערך חשוב ביותר ליחסי הציבור של העסק - דבר שלא תמיד חושבים עליו.

בשלב הראשון, טיטל ולינדרוס מייצעים לבעלי העסקים לכתוב את תוכנית ההמשכיות העסקית. זה אמור להיות מובן מאליו, אבל מסתבר שבהרבה מאוד ארגונים, לא זה המצב. התוכנית צריכה לכלול תיאור של כל התהליכים העסקיים בארגון, הערכת עלויות נזק במקרה של אסון, כולל בהקשר של אובדן ימי עבודה. צריך בנוסף לחשוב על חלופות ריאליות לכל תהליך וכמובן - לתעדף.

יש דברים שחייבים להיות בכל תוכנית: מטרת התוכנית, מוקדים עסקיים רגישים, השפעות קריטיות במקרה של אסון, השלכה הדדית של תקלה, השבתת התהליכים עסקיים שייפגעו על כאלה שלא ייפגעו, הגדרה מדויקת של צפי זמן השביתה, אם זו תקרה, ותוכנית לתחזוקה שוטפת של המערכות התפעוליות.

השלב הבא הוא תרגול, העמדת התוכנית במבחן המציאות. על התרגול להיות מבצעי וצריך לקיים בעקבותיו דיונים בהנהלה. במרבית הארגונים, מדובר בנושא הרגיש ביותר. אחד המנמ"רים בארגון פיננסי סיפר לי לא מכבר שבחצי השנה האחרונה ביצעו אצלם מספר תרגילים, ברמות שונות. אחד מהם היה דילוג פתאומי למתקן חירום ואחר היה במטה החברה, שם ישבו נציגי כל המחלקות העסקיות בחדר אחד במשך 24 שעות ותרגלו "אירועים" שהמנמ"ר והצוות שלו הנחיתו עליהם. במסגרת אחד מהם קיבלו האנשים הודעה מדומה: אין מחשבים, אין תקשורת, תחילתו לעבוד עם ניירות. היה ברור לכולם שללא תוכנית ידועה שהוכנה מראש ותורגלה פנימית על ידי כל המחלקות החשובות בארגון, התרגיל היה נכשל.

כאן אני מגיע שוב לנקודת המוצא: DR או BC. ככל שמחויבות ומודעות הנהלה של הארגון חלשות ודחוקות יותר, כך רמת התוכניות של ההמשכיות העסקית חלשה יותר. או אז, הדבר היחיד שיכול המנכ"ל של אותו ארגון לעשות הוא להתפלל שרגע המבחן לא יהיה במשמרת שלו.

היערכות לשעת חירום והכנת מתקני החירום, DR-ו BC, הפכו זה מכבר להיות חלק מסדר היום של המנמ"רים בארגונים גדולים וקטנים. ההתגברות של הטרור הקיברנטי והטרור העולמי בכלל הכניסה לדיון הזה מושג פופולרי נוסף: סייבר. היערכות לקראת מתקפות הסייבר צמצמה את הדיון הרחב על היערכות למקרי אסון לתחום הצר של ה-DR והיכולת של גורמים חיצוניים לגרום נזק ממשי, פיזי, על ידי פגיעה באתר שבו יושבות מערכות המידע או פגיעה במחשבים עצמם. לעומת זאת, החיבור האוטומטי בין ה-BC ל-DR מגמד מאוד את הדיון ב-BC, תוכנית ההמשכיות העסקית. ברמות המקצועית והארגונית כאחת זה חשוב לא פחות מאשר התוכנית להתאוששות. אף על פי ששני המושגים האלה גרים באותה השכונה, שרשרת המזון מתחילה מ-BC ולא מ-DR, כפי שנוטים לחשוב. כך לפחות סבורים שני מומחים לנושא, אד טיטל וקים לינדרוס, במאמר דעה שפרסמו לא מכבר במגזין המקוון CIO. המשכיות עסקית היא תוצאה של תכנון ארוך טווח, מפורט מאוד, שמאפשר לכל גורם רלוונטי לדעת בשעת אסון מה עליו לעשות וביחד, כקבוצה, להביא לכך שהנזק שנגרם לארגון יהיה מינימלי. ה-DR הוא מרכיב חשוב בתהליך, אבל הוא לא היוצר, אלא הנגרר. ללא ה-BC לא יהיה DR. מנמ"רים רבים יודעים אולי את העובדה הזאת אבל לא מיישמים לאורה ולכן ריכוז מחברי המאמר כמה עצות.

מדוע בכלל תוכנית עסקית היא דבר חשוב? שואלים טיטל ולינדרוס, ומשיבים באמצעות הדוגמה הבאה: נניח שהבניין שבו מערכות המידע נמצא נהרס. העובדים אמורים לעבור למתקן חלופי. אם לא תהיה מראש תוכנית המשכיות עסקית סדורה וברורה, שגם תורגלה, כיצד יידעו העובדים להגיע למתקן החלופי? איך הם יידעו מה תפקידו של כל אחד? תוכנית המשכיות עסקית רלוונטית לעסק קטן כמו לעסק גדול. שניהם עובדים בסביבה תחרותית והיכולת של עסק לחזור לשגרה אחרי מצבים קטסטרופליים תקטין את הסיכון שקיים במצבים האלה: אם הם לא יעשו זאת במהרה, הלקוחות יעברו למתחרים. יש לנראות שבחזרה