

של הארגונים, ועליהם לעבור כברת דרך כדי לממש את היעד. תפיסת ההגנה של החברה, אמר ריבולי, "כוללת רכיבי הגנה על המידע ורכיבי שליטה רבים: ניטור תשתיות, חינוך עובדים, ממשל ז, ניהול סיכונים, הגנה על התשתיות, הגנה על היישומים, הגנה על מכשירים ניידים ואבטחת מערכות האחסון. יש להגן על המידע הקריטי, לקבוע ולממש מדיניות אבטחת מידע ותהליכים, להגן על המשתמשים ולייצר בקרבם מודעות".

הוא סיכם באומרו, כי "ארגונים נדרשים למימוש של ניהול סיכונים תוך שינוי התרבות הארגונית. אנו מספקים כלים הנותנים גידול ביכולת ההגנה, צמצום הסיכונים מבלי להכביד על מערכות ה-IT. ארגונים נמצאים רק בתחילת הדרך של השינוי התפיסתי הזה, ויש להם עוד הרבה מה לעשות בתחום. מדובר בשינוי תפיסתי לא פחות ממה שהיא טכנולוגי".

### "נמשיך לגדול גם ב-2013"

"ארגונים שרויים במצוקה תקציבית לא קטנה, ובהתאם מצמצמים או מותירים על כנם את תקציבי ה-IT שלהם - ובתוכם את תקציבי אבטחת המידע. למרות זאת, נפח הפעילות של סימנטק ישראל גדל באופן משמעותי השנה והוא צפוי להמשיך ולגדול גם ב-2013, אמר **שמוליק אנג'ל**, מנכ"ל סימנטק ישראל.



שמוליק אנג'ל, מנכ"ל סימנטק ישראל

**שמוליק אנג'ל:**  
**"המטרה היא 'חיבוק'**  
**המידע באופן מוגן**  
**לכל אורך חייו. וכמובן**  
**- חשוב שהמידע**  
**יגיע ליעדו ולא לידי**  
**מי שאינם בעליו,**  
**או שאינם מורשים**  
**בגישה אליו"**

"המידע עובר מסלול, כמו המסלול שעוברים הנוסעים והמזוודות בשדה התעופה", אמר אנג'ל בהתאם לרוח האירוע - שעוצב כשדה תעופה ומשתתפיו היו נוסעים לחו"ל לכאורה. "יש לטפל במידע מרגע היווצרו ועד ארכובו", הוסיף, "ולעשות זאת תוך תעודף - כמו שהטיפול בכבודה שבירה שונה מהטיפול במזוודות רגילות. המטרה היא 'חיבוק' המידע באופן מוגן לכל אורך חייו. וכמובן - חשוב שהמידע יגיע ליעדו ולא לידי מי שאינם בעליו, או שאינם מורשים בגישה אליו".

"הדרך שלנו להבטיח לארגונים תהליך נכון של הטיפול במידע והגנה עליו, היא בשילוב של ניהול סיכונים כחלק אינטגרלי בשכבות ההגנה של ה-IT", אמר אנג'ל. "ניהול סיכונים נכון נעשה מלמעלה עד למטה, כאשר ברמה הנמוכה יותר מטמיעים מוצרים שמבטיחים שהמידע יגיע ליעדו - ורק ליעדו".

### "עולם ה-IT | חווה שינויים ותהליכים משמעותיים"

לדבריו, "עולם ה-IT חווה שינויים ותהליכים משמעותיים וארגונים נדרשים להיערך לקראתם. הווירטואליזציה, למשל, נעה במהירות לעבר סביבות ה-IT הקריטיות של הארגונים - מגמה הדורשת מענה בהיבט השליטה והניהול של מערכי המיחשוב, כמו גם היבט אבטחה".

בנוסף, ציין אנג'ל, כי "מגמת ה-BYOD (Bring Your Own Device), תופסת 'הבא את מכשירך מהבית', תופסת תאוצה. הארגונים נדרשים לאפשר לעובדים יכולות עבודה מכל מקום, עם כל מכשיר ובכל עת. תחום המיחשוב הנייד טומן בחובו היבטים רבים של אבטחת מידע: ניהול המכשירים, הקצאת המידע, בקרה למי המידע מגיע, בקרת גישה, היערכות לאובדן מידע ועוד".

במסגרת הכנס הושקו התקנים משולבים של חומרה, תוכנה, מערכות הפעלה, תקשורת וניהול - לגיבוי נתונים וביטול כפילויות. אנג'ל ציין, כי מטרת ההתקנים היא לקדם את מה שגרטרנד מכנה "המצב הרצוי של הגיבוי". מצב זה, הסביר, נוצר בשל ההטרורגניות של מערכות ה-IT, הדורשת להגן על שרתים וירטואליים ופיסיים, כאשר נוצרו פתרונות גיבוי שונים ויש בעיות אינטגרציה בין חומרה ותוכנה. ההתקנים הללו, אמר, מספקים גיבוי משולב, מקצה לקצה - עבור סביבות השרתים, האחסון והתוכנה.



יילי נצר, מנהלת שיווק אזורי, ישראל, קפריסין ומלטה, סימנטק

"מטרתנו", סיכם אנג'ל, "היא לאפשר לארגונים לעבוד בצורה בטוחה ומאובטחת, ללא תלות בתשתיות הספציפיות, ולקיים אינטראקציה מלאה בין המשתמשים ליישומים הארגוניים באופן כלכלי ומאובטח. לכל אחת משלוש מגמות-על בעולם ה-IT כיום - וירטואליזציה, מעבר למיחשוב ענן והתפשטות העולם הנייד - יש לסימנטק מענה, בזכות הרכישות הרבות אותן היא ביצעה בשלוש השנים האחרונות, לצד מחקר ופיתוח פנימיים".

לאחר מכן הכנס התפצל לשלושה מסלולים: פתרונות אבטחת מידע, פתרונות ניהול הענן הפרטי ופתרונות הגנה על נתונים.