

SIEM, ולאגד את המידע המצוי בכלל מערכות ה-IT של גורמי משרדי הממשלה השונים. בדרך זו, אמר, תעלה רמת אבטחת המידע במגזר הממשלתי, ו"על הדרך" תשופר רמת השירותים הממשלתיים.

הוא סיים בצינון כי בשל הקמת מטה התיקשוב הממשלתי, יש כעת ראיית-על לתחום ה-IT במגזר זה, עם ענני מיחשוב, והגנת סייבר.

"אנחנו במלחמה"

"שליש מהמתקפות הקיברנטיות ותקריות הסייבר מכוונות למציאת בקיעים בארגונים במגזר הפיננסי. אין כל ספק - אנחנו מצויים במלחמה", כך אמר **חזי כאלו**, מנכ"ל בנק ישראל. כאלו, לשעבר ראש אגף בשב"כ וראש אגף מיחשוב ומערכות מידע בשירותי בריאות כללית, דיבר בכנס לדברי כאלו, "ישראל מתקדמת בעולם הסייבר, ובתוכה גם בנק ישראל. הסייבר הוא תחום מרכזי שהבנק עוסק בו". הוא ציין כי "הבנק מזוהה כגורם אסטרטגי במדינה ופגיעה בו עלולה לגרום נזק אסטרטגי לכלכלת ישראל. אחד האתגרים בפניהם הוא ניצב הוא למנוע חדירות 'מתחת לראדאר'. אנחנו משקיעים שם לא מעט משאבים ומחשבה. גם הבנקים המקבילים לו בעולם רואים בחדירה את הסכנה המרכזית והאיום המוביל, ולא 'חרבוש' אתרים. זה התרחיש הקשה מכולם".

הוא ציין כי הבנק "כפוף לרא"ם, הרשות הממלכתית לאבטחת מידע בשב"כ, ונמצא תחת רגולציה מחמירה. הבנק משקיע רבות בסייבר מחשש לפגיעה במוניטין ולאובדן אמון הציבור בו. הוא מתמודד עם הרבה אימונים. עלינו לצמצם את הפער בתחום המודיעין, ללמוד לתחקר אירועים ולהפיק לקחים".

עלייה בכמות המדינות המותקפות

כאלו ציטט מחקר של ריזון, שלפיו חלה ב-2013 עלייה של 350% בכמות המדינות שבהן נרשמו אירועי סייבר. בדבריו הוא עמד על ההבדלים בין עולמות אבטחת המידע והסייבר: "בעוד אבטחת מידע עוסקת בצד הפסיבי, של הגנה על מערכות מידע, הסייבר עוסק בכל המרחב הקיברנטי - לא רק במערכות מידע אלא גם במערכות אחרות, כאלה שמשולבות עם ה-IT. המתקפות הקיברנטיות מהוות איום אדיר על כלכלות".

בהמשך אזכר כאלו כמה אירועי אבטחת מידע וסייבר, בהם החדירה למערכות אורנג' בצרפת בחודש האחרון והפריצה שאירעה לפני שנתיים למחשבי קרן המטבע הבינלאומית. הוא ציטט מחקר, שלפיו מספר הנוזקות שפותחו והתגלו ליישומי מובייל של בנקים הוכפל ברבעון הראשון השנה. הוא מנה את השחקנים בזירת הסייבר: מעצמות, מדינות, תאגידים, ארגוני טרור, האקטיביסטים



דורעון קונפנו



חזי כאלו

חזי כאלו: "הבנק מזוהה כגורם אסטרטגי במדינה, ופגיעה בו עלולה לגרום נזק אסטרטגי לכלכלת ישראל. אחד האתגרים בפניהם הוא ניצב הוא למנוע חדירות 'מתחת לראדאר'"



אבירם אייזנברג

והאקרים פליליים. הוא ציין כי יעדי התקיפה הם ריגול, שיבוש מערכות, גניבת כסף, מחאה וטרור קיברנטי. לדבריו, "קיימת זליגה של מידע מהתחום המדינתי-ביטחוני לארגוני מאפיה ופשיעה מאורגנת. ארגונים אלה מתאפיינים ברמה טכנולוגית משובחת וגבוהה, והם עושים שימוש בדארקנט וברשתות שוק שחור מקוונות, בהן הם סוחרים במידע עם ביטקוין. זו מלחמה קשה ולכן הסיכונים הם רבים".

"ארגון שמתבסס על מוצרי מדף - חשוף לאיומים"

"ארגון שמבסס את ההגנה מפני סייבר על מוצרי מדף - אינו מוגן וחשוף לאיומים. עם כל הכבוד וההערכה שיש לנו לכלים הטכנולוגיים, הם יודעים להילחם את המלחמה של אתמול. ההאקרים לומדים להכיר את הכלים האלו והם הופכים לפחות ופחות יעילים", כך אמר **אבירם אייזנברג**, מנכ"ל משותף בחברת GNITE, העוסקת בפתרונות ויינוץ לסייבר לארגונים.

"מרבית ההתקפות בסופו של דבר נעשות בסיוע של גורם פנימי", אמר אייזנברג, "תמיד אפשר לשכנע את העובד הזוטר ביותר עם השכר הנמוך שיסייע בהעברת סיסמאות או מידע לכאורה תמים, מבלי שהוא מודע לכך ובעזרתו מנטרלים את כל השרשרת הטכנולוגית של הארגון".

"הפתרון שאנחנו פיתחנו הוא הגנה מבוססת על ניתוח התנהגות" סיפר אייזנברג, והוסיף כי "יש לנו מערכות המשלבות מלכודת דבש ובינה מלאכותית חכמה מאוד, שחשובה מאוד לסייבר ומזהה את כל החריגות".

אייזנברג גילה, כי "הסטטיסטיקה אומרת שיש דפוס התנהגות קבוע להתנהגות חריגה בתוך הארגון או מחוצה לה ועל סמך זה אנחנו מבססים את יכולת האיתור וההתראה שלנו", וסיכם: "העיקרון שלנו הוא שילוב בין טכנולוגיה ואנשים - מפני שאסור להיות תלויים בטכנולוגיה". יחד עם אייזנברג הרצה גם גיורא רזנצווייג, אחד השותפים בחברה.

אף חברה לא יכולה להיות מוגנת מפני כל סוגי ההתקפות

שרון נימירובסקי, מחברת WhiteHat, סקר את ההתפתחות המהירה של הטרנדים שעסקו באבטחת מידע החל מימי הפירוול, DLP, ועד לעידן ה-DDOS. "ארגונים משקיעים בפתרונות קיימים וטובים בהגנה על הרשת הארגונית אבל לא מפנימים שהסכנה היא באתר האינטרנט שמהווה מטרה להאקרים וכל מיני גורמים", אמר נימירובסקי, והוסיף כי "כיום מדברים על אבדן מידע כתוצאה מרושעות, אבדן לקוחות, כישלון ביישום רגולציה. האמת היא שאף חברה אינה יכולה להיות מוגנת מפני כל סוגי התקפות על האתר", אמר.

WhiteHat נוסדה בשנת 2001 על ידי אחד מפורשי יאהו!. היא מציעה