

על המנהל לשאול את עצמו איפה הגבול, ועל מנהלי האבטחה לבדוק שמה שהם עושים, הם עושים לתועלת הארגון.

"הפער בין ההגנה והתוקפים - הולך וגדל"

"המצב כיום בעולם אבטחת המידע וההגנה מפני הסייבר הוא שהולך וגדל הפער בין רמת האבטחה של ארגונים לבין רמת התחכום של התוקפים. זהו פער שנדרש לצמצם", כך אמר **אופיר זילביגר**, מנכ"ל SECOZ.

זילביגר שימש כיושב ראש הוועדה המקצועית של הכנס. "אנו רואים בבידור", אמר זילביגר, "כי רוב התקציב שמופנה לטובת אבטחת המידע, מושקע בפועל בכיסוי עלי התאנה הרבים של דרישות הרגולטורים השונים, בעוד פחות מדי משאבים מושקעים באבטחה אפקטיבית, זו אשר מביאה לתוצאות וגורמת להעלאת רמת אבטחת המידע בארגונים, כזו אשר תביא להקטנת הפער האמור בין התוקפים ובין הארגונים המתגוננים מפניהם".

"רגולציה זה חשוב", אמר זילביגר, "אבל נדרש, בה בעת, גם לענות על אתגרי האבטחה, ואלה, למרבה הצער, לא קטנים". הוא ציין כי "יש להפריד בין הסיכון הקיים בשל אי ציות לתקן, חוק ורגולציה - ובין ניהול סיכון, אשר עלול להביא לאובדן מידע, לפריצה, או לאובדן כספי או ירידה במוניטין". לדבריו, "הנהלות מתבלבלות בין השקעה כספית גדולה בעולם הציות לרגולציות. גודל ההשקעות בעולם הציות יוצר תחושה כאילו מירב ההשקעה נעשתה בעולם אבטחת המידע, בעוד שלא כך הדבר".

"המטרה שלנו היא לחיות בעולם הדיגיטלי"

גדעון קונפינו, מנהל אבטחת מידע, מטה התיקשוב הממשלתי, אמר כי "במסגרת תפקידנו, אנו מתייחסים למערך המיחשוב הממשלתי ככל עסק. הממשלה זה ביזנס. המטרה של הממשלה היא לתת שירות ללקוחות, שהם האזרחים".

לדברי קונפינו, "אין גבולות בעולם הדיגיטלי, המטרה שלנו היא לחיות בעולם הדיגיטלי, ובמסגרת עולם זה, על האזרח לקבל כמה שיותר שירותים מהממשלה, לקבל את השירותים בצורה מהירה, שירותית ומאובטחת".

במסגרת פעילות אבטחת המידע הנעשית במגזר הממשלתי, אמר קונפינו, "המטרה היא לתת מענה לבעיות שטרם נוצרו. העובדה כי אנו ארגון מותקף היא לא סיבה שלא לעשות או לעשות לאט".

קונפינו הזכיר את אירוע המתקפה שקרה באסטוניה בשנת 2007, עת האקרים רוסים או

פרו-רוסים תקפו את המדינה המרושתת היטב, והביאו להשבתת המערכות שלה ברמה הלאומית "מה שנדרש הוא להביא למצב בו אבטחת המידע אינה נתפסת כמונעת, אלא ככזו אשר מאפשרת עסקית", אמר.

קונפינו אמר כי במסגרת תוכניות האבטחה העתידיות, ככוונת מטה התיקשוב הממשלתי ליצור מערכת ניהול אירועי אבטחת מידע מרכזית,

ויוצר לעצמו תמונה מלאה של האיומים, הרי שיעילות ההגנה תהא רבה יותר", כך אמר **כרמי גילון**, ראש השב"כ לשעבר.

גילון, שמונה באחרונה לתפקיד יו"ר דירקטוריון סייטג'יק, המציעה מערכת לניתוח מודיעין והערכת סיכונים בתחום אבטחת המידע, דיבר במליאה המרכזית בכנס.

גילון הציג עצמו כמי שבא מהעולם הישן, ודיבר עם דף כתוב, ואמר: "אני מעריך אנשים שאומרים שאינם מבינים בתחום מסוים, ולכן עליהם להיוועץ בעת שהם צריכים לקבל החלטות קשות".

"ארגונים נמצאים לא פעם במצב שבו עליהם להשקיע מיליונים באבטחת מידע, הדבר נכון גם לגבי ארגונים מהמגזר הפיננסי, אבל גם ארגוני לואו-טק. זאת, כיוון שלכל ארגון יש את הנכס שלו, והוא המידע".

איזו טכנולוגיה מתאימה לאיזה ארגון

לדברי גילון, "יש טכנולוגיות מצוינות בתחום הסייבר, אלא שאלה אינן מתאימות לכל ארגון. אז שואל עצמו המנהל, אשר נדרש לאשר את ההוצאה התקציבית, 'מה מכל העצים ייצור את היער שמתאים לארגון שלי?' עוצמת האיום והשינויים התכופים במגוון האיומים מסכנים את הארגון ומצד שני, ההגנה מפני איומים אלה יקרה מאוד".

גילון סיפר כי שמע פעם יושב ראש הנהלה של בנק מספר כי אינו מעז שלא לאשר תקציבים לטובת עוד ועוד מערכות הגנה ואבטחת מידע, "הטראומה הגדולה שלו היא שיתקפו אותו בבטן הרכה שלו, במערכות הליבה הבנקאיות".

הדרך לבניית תוכנית הגנה ואבטחת מידע, אמר גילון, כוללת כמה שלבים: האחד, רישום ומיפוי הנכסים הארגוניים, השני, דירוג אותם נכסים ארגוניים לפי מידת הנזק שתיגרם "כי יש אינסוף איומים, ומנגד יש לא מעט מוגבלויות טכנולוגיות". השלב השלישי, לדברי גילון, "הוא בדיקת שוק, אילו סוגי מענה יש מבחינת ההגנה. גם פה הדבר נדרש להיעשות על פי סדרי עדיפויות".

לאחר מכן, אמר ראש השב"כ לשעבר, "יש לשלב בין האיומים ובין אמצעי ההגנה הנדרשים עבורם, ויש ליצור תמונת מצב המכילה שני מימדים אלה, לטובת הצגת תמונת מצב זו למנהל הכספים או מנכ"ל הארגון - על מנת שאלה יאשרו את בניית המענה הנדרש".

"כל מנהל אבטחת מידע בכל ארגון צריך לתפור את חליפת אבטחת המידע ובניית מערך ההגנה המתאים לו", סיכם גילון, "אבל ההחלטה על הקצאת תקציב היא רק התחלת הדרך. נדרש להיות במצב מתמיד של מעקב

אחר השינויים בארגון, כמו גם מעקב אחר האיומים, שמשתנים גם הם בצורה תדירה. לבסוף, יש לערוך בקרת איכות וביצוע, גם עבור המנהלים הבכירים, וגם עבור מנהלי אבטחת המידע. בעבר בשב"כ, כאשר נדרשנו לאבטח דברים חשובים, לקחנו מאבטח והשכחנו אותו על הכספת, זה גם עלה כסף - אבל זה לא עלה רבע ממחירי אבטחת המידע כיום. כלומר,



כרמי גילון



אופיר זילביגר

כרמי גילון: "יש לשלב בין האיומים

ובין אמצעי ההגנה הנדרשים

עבורם, ויש ליצור תמונת מצב

המכילה שני מימדים אלה, לטובת

הצגת תמונת מצב זו למנהל

הכספים או מנכ"ל הארגון - על

מנת שאלה יאשרו את בניית

המענה הנדרש"