דרושה - תפיסה משולבת

תפיסת ביטחון אינטגרטיבית היא המפתח להגנת הסייבר, שכן החשיפה של הארגון לאירועי סייבר אינה נובעת רק מחשיפת מערכות המיחשוב שלו לאיומים דרך האינטרנט, אלא ממגוון רחב של פרצות, פיזיות וקיברנטיות|

ד"ר אל"מ (מיל.) גבי סיבוני

בשנת 1814 טען **פייר סימול לפלס**, שהיה אסטרונום ומתמטיקאי צרפתי, שאם יהיה בידינו את כל המידע, אזי ניתן יהיה לנבא כל אירוע. בפרשנות שלנו, נוכל לנבא בכל הטלת מטבע על איזה צד הוא ייפול. זאת כמובן בהנחה שיש לנו את כל המידע הרלוונטי, דוגמת מבנה מוחלט של המטבע, משקל, לחות, טמפרטורה, הרכב האוויר בסביבה, ועוד אין ספור פרמטרים רלוונטיים. לטענתו, משוואות התנועה הינן משוואות סגורות הניתנות לפתרון והן מאפשרות תמיד ניבוי מוחלט של התוצאה. הכשל היחיד בטענה הזו היה ונותר היעדר היכולת שלנו לאסוף ולנתח את כל הפרמטרים הרלוונטיים לארוע הטלת המטבע ולכן אנו נותרים עם מושגים מעולם האקראיות והסטטיסטיקה.

לא היינו נדרשים לטענה הזו לולא ההתפתחות העצומה של כלים ומתודולוגיות באנליזה של מידע עתק (BIG-DATA). אנו עדים להתפתחות עצומה המאפשרת לאסוף מידע כמעט ללא מגבלות וליכולת לנתח אותו באמצעות כלי אנליטיקה מתקדמים. תחום ביטחון הסייבר הינו אחד הנהנים מהתפתחות מהירה זו. לא רק בהקשרי איסוף מודיעיני, אלא גם בהקשר של הבנת תמונת המצב הלאומית והארגונית של ביטחון מרחב הסייבר. זאת לצד העובדה שהכמויות העצומות של מידע ואירועים ממגוון מקורות ובספיקה עצומה, מציבות אתגר עצום בכל הקשור לניסיון לזקק מתוך מידע זה תמונת מצב רלוונטית, ברורה, רחבה וכוללת.

אחת הדוגמאות המוכרות שממחישות את האתגר הזה היא של קבוצת חוקרים המנסה לזהות פיל באמצעות מישוש בלבד. כל אחד מהם מסוגל לחוש רק את המקטע שמולו, בלא יכולת לגבש תמונה מלאה. כך גם המצב בכלל התחומים ועל אחת כמה וכמה בהבנת תמונת המצב במרחב הסייבר.

לראות את התמונה המלאה

התפוצה של איומים במרחב הסייבר והיכולת של התוקפים לאתר חולשות ולפעול דרכן, מחייבת התבוננות הוליסטית על הביטחון הארגוני. החשיפה של הארגון לארועי סייבר אינה נובעת רק מחשיפה של מערכות המיחשוב שלו לאיומים דרך האינטרנט, אלא ממגוון רחב של פרצות. כך גדלה ההבנה שכדי להבין את המתרחש במרחב הסייבר יש לייצר תמונת מצב אינטגרטיבית מקיפה על המתרחש בארגון, הן במרחב הקיברנטי והן בזה הפיזי. כפי שתוקפים ברמה המדינתית וארגוני טרור אינם מפרידים בין המרחבים, אלא יוצרים מערכה משולבת בין מרחב הסייבר והמרחב הפיזי, כך גם על המגן להימנע מההפרדה מלאכותית בין ההגנה בשני המרחבים העלולה לפגוע בו. מכאן החובה לייצר תפיסת ביטחון אינטגרטיבית המשלבת בין מרחב הסייבר והמרחב הפיזי. אך הבנת תמונת המצב המשולבת הינה אתגר לא פשוט כלל וכלל ומחייבת כלים ויכולות שיאפשרו לנו לראות את התמונה המלאה

> "האתגר המרכזי הוא לייצר היתוך של כל המידע המגיע ממגוון מקורות - מרכזי ביטחון סייבר (SOC), מרכזי ניהול הרשת (NOC), אירועים במערכות המידע והתקשורת (ICT), התראות ממערכות למניעת זליגת מידע (DLP) וכן מידע מכלל מערכות האבטחה הפיזיות של הארגון"

(לזהות את הפיל שבתרשים) ולא רק לזהות חלקים מבודדים שלה (בתרשים: חדק, זנב, חטים).

המידע מגיע ממגוון עצום של סנסורים ומקורות ומאופיין על-ידי שלושה מרכיבים עיקריים התורמים לקושי האמור:

המרכיב הראשון הינו כמות המידע. בבואנו לנסות לייצר תמונת מצב כוללת אנו נדרשים לכמויות מידע עצומות. מידע זה מגיע מכלל המערכות הארגוניות, או הלאומיות.

המרכיב השני הינו השונות העצומה של המידע ומקורות המידע. זהו אתגר עצום - יש לאסוף מידע ממרכזי ביטחון סייבר (SOC), מרכזי ניהול הרשת (NOC), אירועים במערכות המידע והתקשורת (ICT), והתראות ממערכות למניעת זליגת מידע (DLP). ואם לא די בכל אלה, הרי שלצורך השלמת תמונת המצב הכוללת - ומתוך ההבנה העמוקה שלא ניתן להפריד בין ביטחון מרחב הסייבר לביטחון המרחב הפיזי - יש לאסוף מידע מכלל מערכות האבטחה הפיזית של הארגון. לדוגמא, מערכות בקרת הגישה, ניהול הנוכחות ועוד. וגם באלה לא די. מידע מודיעיני הינו קריטי לכל ארגון וכך אנו נדרשים לאסוף מידע מודיעיני ממקורות מחוץ לארגון (רשת האינטרנט על מגוון השכבות שבה) וממקורות פנימיים (התנהגות עובדים, מאפייני פעולה של תחנות קצה ועוד).

המרכיב השלישי המאפיין את המידע הינו קצב הייצור וזרימת המידע. השילוב בין שלושת המרכיבים האלה - כמות, שונות וקצב, מייצר אתגר מהותי ביכולת לייצר תמונת מצב איכותית ורלוונטית לביטחון הארגוני או הלאומי.

האתגר המרכזי בבניית תפיסת בטחון אינטגרטיבית הוא לייצר היתוך של כל המידע ויצירת מתאם בקצב, שיאפשר לתובנות שיגזרו מהיתוך זה להיות רלוונטיות לסיכול האיום.

מעגל הסיכול והמניעה

מעגל הסיכול צריך לכלול לפחות ארבעה מאמצים: הראשון שבהם הינו היכולת לייצר התרעה (Early Warning). על ההתרעה להיות קונקרטית ורלוונטית על מנת שתאפשר פעילות תגובה ממשית. בדרך כלל, ראוי לקבוע מדרג התרעות עם מדרגי תגובה המתאימים לכל חומרת התרעה. מאמץ המניעה (Prevention) הינו המרכיב השני ועניינו הפעולה האקטיבית הארגונית, או הלאומית, למנוע מהאיום להתממש. מאמץ הגילוי (Detection) הנו מאמץ חיוני שמטרתו להבין באיזו מידה הארגון נפגע ונחדר. ולבסוף, מאמץ התגובה (Reaction). תפיסת הסיכול מחייבת, כי מאמץ זה לא יעסוק רק בפעילות "רועשת", או "שקטה", לעצירת פעולת התקיפה, אלא גם שימוש בתקיפה, במסגרת מאמץ איסוף מודיעין ואף היפוך היוצרות למצב בו הרודף הופך לנרדף.

גדלה ההבנה, כי מרחב הסייבר לא יוכל להיות מרחב פעולה מבודד, עצמאי ו"חוצני". ההתמודדות עם התעצמות האיומים מחייבת תפיסת ביטחון אינטגרטיבית, המשלבת בין המרחב הקיברנטי לזה הפיזי, וכל ניסיון לקבע את ההפרדה הזו הינו מלאכותי ומועד לכשלון.

הכותב הינו ראש תוכנית בוטחון סייבר במכון למחקרי ביטחון לאומי