בין מתודולוגיה לטכנולוגיה

התרחבות איומי הסייבר, ברשת ומחוצה לה, מחייבים איסוף עקבי של מידע מכל המקורות האפשריים בארגון, תוך תחקור ואנליזה שיטתית להצגת תמונת מודיעין מלאה. כמענה לאיומים החדשים מציעה חברת טלדור, שפועלת בשנים האחרונות בעוצמה בתחום הסייבר, שילוב של מתודולוגיות מודיעיניות, יחד עם טכנולוגיות אבטחת מידע פורצות דרך ויכולות גבוהות של טיפול ב-Big Data | **אביגיל דנה**

התפתחות המואצת של תעשיית הסייבר הישראלית בשלוש השנים האחרונות מיוחסת, בין היתר, להטמעה של ידע וטכנולוגיות מעולמות המודיעין הביטחוניים במגזר העסקי. הרבה מאוד ממתודולוגיות המודיעין הצבאי חדרו לתחום אבטחת המידע המסורתי ומונחים כמו "איסוף", "הרכשה", ו"תחקור של מידע ממקורות גלויים" הפכו לחלק מהעגה המקצועית בסייבר. חברות שכבר היו פעילות במערכת הביטחונית הצליחו לתרגם מהר יותר את הידע שצברו לטובת המגזר העסקי. אחת מהן, ואולי המובהקת ביותר, היא חברת טלדור, מהחברות המובילות בתחום טכנולוגיות המידע ותפעול מערכות מידע עם ותק של 25 שנה.

"נכון שהניסיון שצברנו במערכות הביטחוניות סייע לנו מאוד לפתח את תחום הסייבר, אבל הפעילות שלנו בתחום היא רחבה יותר מאשר אזרוח טכנולוגיות ביטחוניות", אומר **רני קהת**, סמנכ"ל מכירות בתחום הגנת הסייבר בחברה. "היכולת של טלדור להעניק לקשת רחבה של ארגונים מעטפת הגנה חדשנית ויוזמת המותאמת לצרכיהם, נגזרת, בראש ובראשונה, מההבנה שלנו בתהליכים עסקיים שונים והשלכותיהם".

קהת מוסיף, כי החברה גם יזמה שורה של פעולות כדי לקדם את התחום: "הקמנו מעבדות סייבר ומתחמים מסוגים, ערכנו סדנאות להעלאת מודעות לנושא אבטחת המידע בקרב לקוחותינו, פיתחנו אינטגרציית פתרונות סייבר ואבטחת מידע בענן, קלטנו והכשרנו עובדים ייעודיים לתחום ורשמנו יישום מוצלח של למעלה מ-20 פרויקטי אבטחת מידע וסייבר".

לדבריו, טלדור התאימה את עצמה במהירות לעולם אבטחת המידע החדש, שכולל גם מערכות ניהול ובקרה של בניינים, מערכות הקלטה ומערכות פיזיות כגון בקרת כניסה, כרטיסי עובד, מצלמות ועוד על מנת לקבל תמונת מודיעין שלמה ומקיפה. יכולות אלה מתורגמים למוצרים ושירותים הן עבור המגזר הביטחוני והן עבור המגזר הפיננסי, וכן עבור שורה של חברות עסקיות, לרבות חברות קטנות ובינוניות.

כיום, שירותי אבטחת המידע של טלדור כוללים, בין היתר, תכנון ויישום של אסטרטגית אבטחת מידע ארגונית, בחינת יישומים למניעת פרצות וסיכוני אבטחת מידע, ניהול זהויות, תפעול ושמירה על מידע פרטי בכפוף להנחיות רגולטוריות, אבטחת שירותי אינטרנט, פיתוח עמדות הלבנה, תכנון המשכיות עסקית, מניעת זליגה של מידע וניתוח אירועי פריצה ואיתור המקור לפריצה.

יכולות חזקות ב-Big Data

דדי גרטלר, אחראי על פיתוח עסקי לתחום המודיעין והסייבר בחטיבה הביטחונית בטלדור, מאשר כי הניסיון של החברה ביישום והטמעת מערכות מודיעין במגזר הביטחוני (SIGINT ו-WEBINT) אפשר לה לפתח מערכות מודיעין לעולם הסייבר לטובת חיזוק קווי ההגנה של ארגונים ממשלתיים וחברות, הזקוקות לשכבת הגנה חזקה במיוחד, המורכבת מיישומי ומערכות אבטחה ייעודיים. אך לכך הוא מוסיף שני רכיבים נוספים - יכולת איסוף והרכשה של מידע גם בתוך הארגון ולא רק מחוצה לו כגון, בשרתים, באפליקציות ובכל רכיבי התקשורת לצד היכולות החזקות של החברה בתחום אחסון, ניהול ועיבוד מידע של Big Data.

"לטלדור ניסיון מוכח בתכנון ויישום פתרונות Big Data", מדגיש גרטלר, "הן בבנייה, הן בטכנולוגיה והן בארכיטקטורה, תוך מימוש של פתרונות Big Data מבוזרים, שרובם מבוססים על טכנולוגיה של קוד פתוח, כגון Hadoop ו-NOSQL Databases. אנו יודעים להתמודד עם כמויות אין סופיות כמעט של נתונים מגוונים ולבחון כל סוג של קובץ - טקסט, תמונה, או וידיאו - ולסרוק כל שרת, נתב או מתג בשגרה שוטפת וקבועה, על בסיס אלגוריתמיקה שפותחה ורצה על המידע, תוך ביצוע תחקיר ואנליזה בצורה יעילה ומהירה. התוצאה היא מתן התראות על אירועים חריגים ועל פוטנציאל האיום".

מענה מקיף

בסקר האחרון של חברת האנליסטים STKI קיבלה טלדור את הדירוג הראשון מבין האינטגרטורים במכירות אבטחת מידע וסייבר, והשני מכלל הספקים, אחרי סימנטק. בחברה רואים בכך עדות נוספת ליכולות של החברה בתחום הסייבר ומציינים, כי החברה מעניקה כיום מענה מקיף לצרכי אבטחת המידע של הארגון, החל מפתרונות תשתיתיים שמגנים על ליבת מערכות אחסון, דרך בסיסי נתונים, מערכות הפעלה וטלפוניה, ועד לפתרונות אפליקטיביים עבור היישומים המצויים בשכבות המחשוב העליונות.

"העובדים המומחים שלנו הינם בעלי הסמכות בין-לאומיות ועשרות שנים של ניסיון מצטבר באבטחת מידע, ועוברים הכשרות רלוונטיות על בסיס תקופתי", מסכם רני קהת. "הם מסוגלים להעריך את רמת הסיכון הנדרשת לכל רכיב במערכות המידע ומעצבים פתרון כולל לכל אתגרי האבטחה של הארגון, המורכב מהמיטב שיש ליצרנים המובילים ולטלדור להציע".

ארבעה איומים מרכזיים

באגף הסייבר של חברת טלדור ביצעו לאחרונה ניתוח מקיף של האיומים המרכזיים הצפויים בתחום בשנתיים הקרובות:

1. איומי ה-BYOD בתחום המובייל - להערכת החברה, בגלל אי-יכולת הקשחת מכשירי הקצה (לא ברמה הטכנולוגית, אלא ברמת הארגון ושיטות), עובדים ולקוחות אינם מוכנים להוריד מיכולות וביצועי המכשיר לטובת אבטחה. לכן הפתרונות יהיו יותר בכיוון של כתיבת אפליקציות מוקשחות, והצבת "שומרי סף" (gateways) שיהיו במרכז המערכת. ההנחה היא שככל שתהיה נגישות לשירותים שונים דרך הטלפונים החכמים, כך תגבר רמת התחכום של רוגולות ונוזקות למיניהן שיכתבו למכשירי הקצה. החברה נערכת בהתאם עם אמצעי אבטחה לשירותים ואפליקציות נגישות דרך מכשירים סלולריים, כאשר המטרה היא ליצור פתרונות clientless - כלומר, תוך התערבות מינימלית במכשיר הקצה.

2. התקפות חברתיות - בטלדור מעריכים כי נראה יותר גניבת זהויות, פשעי סייבר, מעילות כספים והונאה ברשתות החברתיות למיניהן. בתחום זה מציעים בטלדור יכולות מוכחות בתחום איסוף מודיעין בסביבה הקבירנטית.

3. עלייה בנוזקות שמנסות לגנוב מטבעות וירטואליים ומעילת כספים - ההערכה היא שנהיה עדים ליותר ויותר ניסיונות לבצע סחיטה על מידע שנגנב או הוצפן במערכות הקורבן, כדוגמת תוכנת cryptolocker שביצעה נזקים רבים ב-2013. צורת התקפה זו ניתן לעצירה בקצוות הרשת ובטלדור ערוכים לכך עם פתרונות מתאימים.

4. הגברת האיומים בענן השירות - לאבטחת מידע בענן יהיו עלויות אבטחה כבדות כגון שימוש בהצפנה, ניהול תעודות דיגיטליות, אמצעי הזדהות חזקים ועוד. זהו עולם מורכב ובטלדור מייעצים ללקוחות באשר ליתרונות וסיכונים שכרוכים בפעילות ענן.

רק הקטנות יכולות

אחת מההתפתחויות שעליהן גאים בטלדור במיוחד היא זיהוי ואימוץ טכנולוגיות חדשניות של חברות סטרט-אפ ישראליות הפועלות בתחום הסייבר, תוך שילובן במערך הפתרונות של החברה ובפתרון השלם ללקוחות. זה היה גם אחד הנימוקים בהם השתמש חבר השופטים, שזיכה את טלדור באות הוקרה על תרומתה לקידום ענף הסייבר ואבטחת המידע.

"פיתחנו פלטפורמה לעידוד השקעות בסטרט-אפים, מתוך הבנה שהחברות הקטנות והזריזות הללו יודעות לזהות פגיעויות ולספק פתרונות בצורה מהירה הרבה יותר מאשר החברות הגדולות", אומר ניר שפריר מנהל תחום פיתוח טכנולוגיות מתקדמות . "עולם הסייבר הוא דינאמי ואנו נדרשים ליכולות חדשות שהתאגידים הגדולים בתחום אבטחת המידע מתקשים להשיג".

בין השאר, שפריר מתייחס לדור חדש של מוצרי אבטחה שפועלים גם בתחנות קצה וגם ב"שומרי השער" (gateway) שיעלה לאוויר ב-2014 ומובל על-ידי חברות סטרט-אפ. חברות אלו גם מובילות בזיהוי אפליקציות ותוכנות זדוניות על סמך "רשימה לבנה". כלומר, לאחר התובנה שלא ניתן לזהות תוכנה זדונית באמצעות חתימה ("תעודת הזהות" של התוכנה) הרי כמו קצין ביטחון טוב, יש לתחקר ולתשאל את התוכנה בשער הכניסה ולא רק לסמוך על תעודת הזהות. דור זה מתבסס על טכנולוגיות חדשות כדוגמת "ארגז חול" (sandbox), בהרצת הקוד עצמו ואמולציות שונות, כולל אמולציות חומרה של המעבד שמריץ את הקוד.

מדובר בחברות כגון Hybrid security, שמשווקת על-ידי טלדור וחברת Nyotron, שמפתחת דור חדש של מניעת פעולות זדוניות בתחנת הקצה באמצעות זיהוי פעולות לא מורשות ברמת הקוד, שהן רמות מאוד נמוכות של מערכת ההפעלה.