

איך רותמים את Big Data למודיעין אבטחה

אחת ההבטחות הגדולות הגלומות ב-Big Data היא שיפור האבטחה הכוללת בארגונים, ומתן האפשרות לחזות בצורה פרואקטיבית את רמות הסיכונים ואת המקומות שבהם דברים עלולים להשתבש • ניהול סיכונים אבטחה בעידן הביג דאטה

ד"ר אייל קולמן ואלכס וייסטיך *

לארגונים להשתמש באבטחה מבוססת מידע על מנת להפחית את הסיכון הכולל - כבר קיימת. באופן ספציפי, ספקים של טכנולוגיות לניהול תקריות ואירועי אבטחה, מאמצים מגמה זו באמצעות הוספת פלטפורמת ניתוח להיצע שלהם, ושילוב עם מקורות מידע רבים מתמיד.

לדוגמה, ניתן לשלב נתוני מיקום של המשתמשים ממקורות רבים, כולל הרשת הארגונית, רשתות Wi-Fi המשמשות לעבודה מרחוק, נתוני מיקום מתוך המכשירים הסלולריים, מערכת דיווח השעות, דיווחי הנסיעות ועוד. הצגת נתונים אלו והצלבתם עם מקורות מודיעיניים מאפשרת הבנה מלאה ומדויקת יותר של מצב הארגון (לדוגמה, מי נמצא איפה), גילוי

מוקדם של התקפות מבוססות התחזות, והערכה של סיכונים עתידיים אפשריים. המידע קיים במלואו או ברובו אצל החברות, צריך רק להשתמש בו בצורה מועילה.

אחת ההבטחות הגדולות הגלומות ב-Big Data, היא שיפור האבטחה הכוללת בארגונים, ומתן האפשרות לחזות בצורה פרואקטיבית את רמות הסיכונים ואת המקומות שבהם דברים עלולים להשתבש. ניתוח אבטחה מבוסס מידע צריך להוות שיקול מרכזי במדידת סיכונים אבטחת מידע ויש להעניק לו תשומת לב ברמה הניהולית, ממש כשם שהנהלות מעריכות סיכונים תפעוליים כוללים. ארגונים שלא יאמצו ניתוח אבטחה מבוסס מידע, יהיו חשופים במידה רבה יותר לנזקים כלכליים ותדמיתיים חמורים.

ב-RSA ישראל יושבת מחלקת ה-Data Science העולמית של RSA בראשות ד"ר אלון קאופמן. הקבוצה אחראית על המחקר בתחום של פתרונות אבטחה מתקדמים מבוססי למידה חישובית בעולם ה-Big Data. הקבוצה מונה כ-15 חוקרים, מומחי אבטחה ומהנדסי Big Data. ותוצרי הקבוצה מיושמים במגוון רחב ממוצרי RSA. מטרת המחקר והפתרונות המפותחים בישראל הינם לייצר אבטחה משופרת לארגונים באמצעות יכולות זיהוי מהירות יותר ומדויקות יותר של התקפות ידועות או שאינן ידועות, ויעול הטיפול בהתקפות שנתגלו. אחד התחומים הבולטים ב-RSA ישראל הינו מניעת הונאות פיננסיות.

* ד"ר אייל קולמן, ראש צוות Data Science למגזר הארגוני ב-RSA, חטיבת האבטחה של EMC; אלכס וייסטיך, מומחה אבטחה וארכיטקט Data Science ב-RSA.

כל עסק מתמודד עם סיכונים. אולם עסק שרוצה להיות חדשני ולייצר ערך עבור הלקוחות ובעלי המניות שלו, צריך לא רק להתמודד עם הסיכון, אלא לאמץ אותו ולנהלו באופן יעיל. אנו חיים בעידן שבו רשתות המחשבים מתרחבות בהתמדה, לצד עלייה ניכרת במגוון מקורות הנתונים ובנפחם. את הנתונים הללו ניתן לרתום לטובת שיפור מודיעין האבטחה ויכולות ניהול הסיכונים של הארגון.

ארגונים משתמשים כבר זמן רב בבינה עסקית כאמצעי להפוך נתונים גולמיים למידע שניתן לפעול על בסיסו, ומסוגל לסייע בזיהוי הזדמנויות חדשות ומקסום רווחים. עם זאת, בכל הנוגע לתחום האבטחה, השימוש בבינה

עסקית, או בכלי מדע נתונים, Data Science - עדיין לא נפוץ מספיק. הכלים והמידע הנכונים מאפשרים לחשב סיכונים, לשלוט בהם ולנהל אותם, לחשוף דפוסים של סיכונים על מנת לחזות אירועים ולשפר את הביצועים הכוללים. שימוש בתובנות המתקבלות מתוך ניתוח הנתונים שהארגונים מייצרים, מקנה יתרון תחרותי ויכולת לנהל סיכונים בצורה פרואקטיבית יותר.

נפח הנתונים בכל ארגון הולך וגדל במהירות ככל שהשימוש בטכנולוגיות תקשורת ומידע ממשיך לגדול, וסוגים חדשים של מערכות ומכשירים - מטלפונים סלולריים ועד ציוד תעשייתי - מתחברים לרשתות הארגוניות. הכמות האדירה של הנתונים שהארגונים מייצרים, הולידה את הביטוי Big Data. בחברת המחקר מקינזי מעריכים, כי כמות הנתונים המיוצרים מדי שנה בעולם עולה

בשיעור של 40%. קצב הצמיחה של המידע שמייצרים ארגונים וחברות מהיר אף יותר, וחברת המחקר פורסטר העריכה כי הוא עומד על 94% מדי שנה.

מאות ואלפי מקורות נתונים

בארגון טיפוסי ישנם מאות, אם לא אלפי, מקורות של רישומי נתוני אירועים, אשר נוצרים על ידי כל מכשיר או מערכת בכל פעם שמתרחש אירוע. הרישומים הללו חיוניים בזיהוי התנהגות חשודה, חשיפת אימים ופרצות, מניעת תקריות אבטחה ותמיכה בניתוח פורנזי. על מנת להפוך רישומים של נתוני אירועים למודיעין משמעותי, צריך לא רק לפקח על האירועים אלא גם ליצור ביניהם מיתאם ולנתח אותם בכלים מתקדמים, כך שאפשר יהיה לחשוף את משמעותם. בעוד שניתוח מבוסס Big Data לצורכי אבטחה עדיין נמצא בשלבים ראשוניים, הטכנולוגיה שתסייע

