

# שימוש בטכנולוגיות מידול וסימולציה לחיזוי התקפות סייבר ארגוניות

אורי לוי, מנהל אזורי EMEA, סקייבוס סקיריטי

הטיפול וההשפעה של האירוע היו קטנים יותר. תפיסה זו עומדת בבסיס הפתרון שחברת סקייבוס מציעה ללקוחותיה בתחום ניהול אבטחה פרואקטיבי לארגונים.

## לחזות את העתיד, להשפיע על ההווה

אם כן, כיצד ניתן לבצע חיזוי של התקפות ואירועי אבטחה עוד לפני שהם קרו? חשבו על פיתוח של מטוס קרב חדשני, לפני שהמטוס נבנה, מפתחי המטוס משתמשים במודל הנדסי של המטוס ובתרחישים שונים ומשונים על מנת לבחון את ביצועי המטוס ואת העמידות שלו באותם תרחישים וזאת עוד לפני שבורג אחד הוברג בגוף המטוס. באופן דומה, הטכנולוגיה של סקייבוס מאפשרת לארגונים לייצר מודל של הרשת הארגונית בצורה

קלה ומהירה תוך "יבוא" מידע סטנדרטי אשר קיים בכל רשת ארגונית (קבצי הגדרות של נתבים ומתגים, חומות אש, מערכות ניהול נכסים, תוצאות סריקה של VM וכו'). מודל זה מכיל את מפת טופולוגית הרשת, את הגדרות הניתוב והמיתוג, את הגדרות האבטחה באמצעי האבטחה השונים ואת השרתים ותחנות העבודה הארגוניות ותחנות העבודה הארגוניות הכוללות גם את הפגיעויות והחולשות הידועות שלהם. כלל המידע הזה מודל למודל אנליטי אשר על גביו מבוצעים ומורצים סימולציות התקפה המאפשרות

להסיק כיצד ניתן לתקוף את הארגון באופן הקל ביותר ולהשיג את האפקט הרב ביותר. אנליזות אלה עונות על שאלות מהותיות לאבטחה הארגונית השוטפת למשל: היכן קיימות הגדרות מוטעות אשר מייצרות חשיפה אבטחתית? אילו חולשות ניתנות לניצול בפועל ולכן עליהם להיות מתוקנים באופן מיידי? מה ההשפעה של איום חדש שהתגלה על הרשת הארגונית שלי? וכו'.

היתרון הגדול הוא שאין שום הפרעה לרשת הארגונית, המידע נשאב באופן שקוף (read only) ממערכות הניהול השונות בארגון ומוזן לתוך מודל הרשת אשר רץ באופן עצמאי על שרת נפרד. מודל זה מאפשר לבצע ניתוחים ותרחישים אוטומטים אשר התוצר שלהם נמסר בצורה של דו"ח (למטרת תאימות למדיניות לדוגמה) או למשל התרעה למרכז תפעול האבטחה (SOC) על נתיב התקפה פתוח ברשת אשר מאפשר ניצול מיידי על ידי תוקף פוטנציאלי.

המערכת מאפשרת לארגונים להפוך להיות פרואקטיבים ולהקטין באופן דרמטי את החשיפה שלהם ואת רמת הסיכון בה הם פועלים. כמו כן היא מקטינה את עלויות האבטחה המושקעות על ידי הארגון, כיון שניתן להתמקד בצורה מדויקת אך ורק בחולשות, נתיבי התקפה וכשלי מדיניות אשר מייצרים סיכון אמיתי ומשמעותי לארגון ולא בצורה גורפת ו'עיוורת' ללא הבחנה בין עיקר לטפל.

אין צורך להכביר מילים בדבר מלחמת הסייבר העולמית המתפתחת ומתדפקת על סף דלתותיהם של ארגונים, ממשלות וגופים ציבוריים. ההתלכדות של מספר מגמות ותהליכי עומק אשר התרחשו בשנים האחרונות וכניסת טכנולוגיות כגון ניידות מחשובית וירטואלזציה, כמו גם חיבור וקישוריות של שירותים ציבוריים וממשלתיים לרשת האינטרנט, הפרו בצורה משמעותית את מאזן הכוחות בין היכולת להגן על תשתיות ושירותים אלו לבין היכולת להתקיף ולשבש את אותם שירותים.

## הפרת מאזן הכוחות

כשבאים לבחון את גל התקיפות והאירועים האחרונים על רקע מאזן הכוחות והמשאבים שבין הכוחות המגינים והכוחות התוקפים, ניתן להבין עד כמה אנו רואים רק את קצה הקרחון.

רוב הארגונים כיום נמצאים בתת איש של מומחי אבטחת מידע, הם מבצעים אך ורק צעדי הגנה הכרחיים ובעיקר כתגובה על צעדים התקפיים שמבוצעים נגדם (יחס של 1 ל-30). מולם עומדים מאות ואלפי תוקפים פוטנציאליים אשר מפעילים מגוון כלים ושיטות התקפה במגוון רחב של קטורי תקיפה החל מניצול חולשות ידועות בתוכנה דרך ניצול טעויות קונפיגורציה רשתיות וכלה בניצול חולשות אנושיות וטעויות (social engineering).

מעולם בהיסטוריה האנושית לא היה חוסר איזון חריף כל כך ביכולת של תוקף 'חלש' לגרום לנזק אדיר כל כך לכח מגן 'חזק' כל כך. הפער הזה מתעצם בכל מימד שבוחנים אותו הן בהשקעה הנדרשת לביצוע התקפה מול ההשקעה הנדרשת בבלימתה והן בנזק הכלכלי שייגרם בגין אותה התקפה לצד המותקף (business impact).

אל הסביבה הזו אנו מטילים מספר משתנים נוספים אשר מחמירים את תמונת המצב עוד יותר. רמת המורכבות של רשת ארגונית כיום היא בסדר גודל אחר מזו שהייתה אך לפני שנים מספר, קצב העדכונים הטכנולוגיים גובר והולך ועמם גם כמות הפגיעויות והאיומים הנגזרים מכך (לדוגמה ניתן לבחון את הזמן בין שחרור תלאים של היצרניות הגדולות בהשוואה לשנים עברו). הדרישות לשינויים ולהתאמת הטכנולוגיה לשינויים בסביבה העסקית ובהעדפות השוק, מגבילות בצורה משמעותית את היכולת של הארגונים להגן ולאבטח את השירותים העסקיים בצורה אפקטיבית ויעילה.

## ההגנה ריאקטיבית להגנה פרואקטיבית

מן הסתם התמודדות ארגונית עם איומי הסייבר השונים הינו תהליך רב שכבתי המכיל מספר רכיבים כגון מדיניות, טכנולוגיה, כח אדם, מתודולוגיה וכו'. בבסיס תפיסת ההגנה הנכונה מבוססת ההנחה כי הצד המגן נמצא בנחיתות מתמדת בכל מימד אפשרי, ולכן הוא חייב להפעיל כלים ושיטות יעילות יותר מהצד התוקף על מנת להתמודד עם רמות האיום הקיימות בצורה אפקטיבית ולא פחות חשוב כלכלית והגיונית לרמת הנזק הפוטנציאלי שיכול להגרם כתוצאה מהתקפה.

מחקר שבוצע לפני מספר שנים מצביע על קשר ישיר בין זמן גילוי וטיפול באירוע אבטחתי לבין העלות הכלכלית הקשורה בו. ככל שהאירוע התגלה בשלב מוקדם יותר (עד כדי מניעה וסיכול) כך העלות הכלכלית של

