

הצורך בשיתוף פעולה וב – Machine Learning

בשנתיים האחרונות אנחנו עדים לעליה משמעותית בהיקף מתקפות הסייבר וברמת התחכום שלהן.

החל בתקיפה שהשביתה את רשת החשמל באוקראינה, עבור בגניבת עשרות מיליוני דולרים בפריצת הבנק בבנגלדש, תקיפת רשת SWIFT (הרשת הגלובלית לטרנזקציות בנקאיות), עבור בתקיפת ה-DDoS שהשביתה את ענקית שירותי ה-DNS חברת DYN, דרך דליפת נתוני אשראי של עשרות מיליונים בתקיפת חברת Equifax, ועד תקיפות יומיומיות של מערכות IOT, מתקפות Ransom, ומתקפות על שירותי חברות במגוון תחומים. נוסף לכך את פרסומי הפריצות האחרונות למערכות ה-NSA בארה"ב וגניבה של כלי תקיפה (Cyber Attack Hacking Tools), שעד כה היו בשימוש ארגונים ברמת מדינה בלבד, וכעת מופצים לשימוש של גורמי פשיעה, האקרים וכנופיות רשת.

מתקפות הסייבר נוגעות בכל תחומי חיינו; אנרגיה ותשתיות, פיננסים ואשראי, רשת האינטרנט עצמה, תחומי הבידור ועוד.

אם בעבר מרבית המתקפות נעשו לצרכי ראווה והצגת יכולות - Show off או גרימת נזק על ידי קודים זדוניים כגון וירוסים ותולעים למיניהן, הרי שבימים אלו רובן המוחלט של המתקפות מבוצע לצרכי רווח. אנו עדים לאבולוציה בה המתקפות הופכות מתקיפות אבטחה וסייבר לתקיפות שתכליתן הונאה - **From Cyber-attacks to Fraud incidents**.

רמת אבטחת ה-Perimeter עלתה פלאים, אך מתקפות המכוונות לבטן הרכה, ישירות לשירותים ולמוצרים (Layer 7 Attacks) עדיין לא מקבלות מענה מלא וראוי במרבית הארגונים.

על מנת לתת מענה לתקיפות מתוחכמות אלו המנצלות חולשות אפליקטיביות, הן בשירותים הפומביים שמספקות חברות והן במערכות הפנימיות, יש צורך לאתר את המתקפה משלביה הראשוניים, לעקוב אחר התפתחותה ולמנוע את הוצאתה לפועל. במשחק החתול והעכבר של עולם אבטחת המידע והגנת הסייבר, **היתרון עומד לצד התוקף!** ככל שהטכנולוגיה מתפתחת, איזור התקיפה גדל ואיתו האפשרויות העומדות בפני התוקף. בד בבד, המורכבות הגדלה יוצרת אתגר משמעותי בפני המגן.

לאחר בחינה מעמיקה של מומחי אבטחת המידע והסייבר ב-WE-Ankor, אנו מבחינים בשני אלמנטים מחייבים המשפרים את רמת ההגנה באירגון:

הצורך בשיתוף פעולה בין הגורמים השונים בארגון העוסקים בנושא – צוותי אבטחת מידע וצוותי מניעת ההונאות יחד עם צוותי ניהול הסיכונים, הגנת הפרטיות והרגולציה. שיתוף פעולה הנשען על שימוש במערכות הגנה המאפשרות קבלת תמונת מצב שלמה וכוללת על ידי הגורמים הרלוונטיים השונים בארגון.

הצורך בהרחבת השימוש בכלים ומערכות המאפשרים ניטור מתמשך, איתור ארועים חריגים והכוללים יכולות התפתחות ולמידה – Machine Learning ויכולות אנליטיקה.



חטיבת אבטחת המידע והסייבר בווי אנקור פועלת על מנת ליצר איזון עדין בין שמירת רמת אבטחה גבוהה לבין הקפדה על חווית לקוח איכותית.

פעילות החטיבה מתמקדת בשלושה תחומים עיקריים:

מערכות ניטור ובקרה

הרחבת פעילות הטמעת מערכות New ArcSight כולל המודולים החדשים המאפשרים פעולות אנליטיות משופרות ומנועי Big Data. המערכות מאפשרות ניטור ואיתור ארועי אבטחה בזמן אמת, יחד עם יכולות מודיעין (RepSM) משופרות ויכולות תחקור וניהול. הטמעת מערכות תומכות ומשיקות – מערכות ניהול אירועים, אוטומציה, מערכות תחקור MSSP – הרחבת אספקת שירותי אבטחה כשירות. שירותי SIEM וכן SOC מנוהלים, כשלצדם שירותים נוספים כגון הגנה מפני Phishing, סינון תוכן דוא"ל וקבצים כשירות ועוד.

Security Big Data - BI ורתימת יכולות Machine Learning

שימוש במערכות Elastic Search, Logstash, Kibana לשיפור יכולות איתור אנומליה בהתנהגות משתמשים/לקוחות, שיפור יכולות הדיווח (Reports) ויכולות הויזואליזציה של ארועי אבטחה לצורך קבלת תמונת מצב מלאה בזמן אמת.

מערכות חדשות 'קלאסיות' לאבטחת מידע והגנת הסייבר

הטמעת מגוון מערכות Cloud Security להגנה על פעילות הארגון ולקוחותיו בענן. שימוש במערכות EDR ומערכות Network Security מתקדמות לאבטחת תשתיות המחשוב של הארגונים והלקוחות.

בעידן זה של שיפור משמעותי בכמותן ובאיכותן של תקיפות הסייבר, עלינו לפעול בתחכום וביצירתיות ולשאוף להדביק את קצב ההתפתחות של התוקפים ואף להשיגם. ניתן לעשות זאת תוך שימוש חכם ויעיל במערכות ובתהליכים הכוללים יכולות Machine Learning שיאפשרו לנו לתת Fight לכלי התקיפה ועם זאת לספק ערך מוסף ללקוחותינו בשמירת סביבת עבודה בטוחה ומהימנה תוך שימור רמה גבוהה של חווית המשתמשים והלקוחות.



לפגישת יעוץ לחץ כאן

מאת: גון קמני, מנהל חטיבת אבטחת מידע וסייבר, ווי אנקור