

המהפכה הבאה בעולם הסייבר כבר כאן

לו יכולנו לשוב בזמן, כשנתיים לאחור ולהציב בפני מנהלים שאלה על מידת ההשפעה של אירועי סייבר על הארגון אותו הם מנהלים, הם היו משיבים, קרוב לוודאי, שהנושא אינו נוגע להם. היום, נשמע תשובות שונות לגמרי. האירועים שזעזעו את העולם המערבי בשנים האחרונות ועיצבו את השינוי בתפיסת העולם של מנהלים את אירועי הסייבר ואיומיו, כללו בין היתר את ההתקפה על **משרד הרשומות האישיות** (סוכנות אמריקאית המנהלת את המידע על עובדי המדינה האמריקאים), חברת **Sony**, חברת **Target** וחברת **RSA**. בהתקפות אלו נגנב מידע רשמי מסווג ונגרמו נזקים ישירים ועקיפים בהיקפים של מאות מיליוני דולרים. ניתן להעריך, שמלבד המידע המפורסם ברבים על התקפות, בין שהצליחו ובין שנבלמו, התקפות רבות נותרו חסויות, משום שלא נתגלו, או שלא דווחו ע"י הנפגעים. לבד מהתרומה המהותית להגברת מודעות המנהלים (העובדה שמנהלים בכירים ובכללם מנמ"רים שילמו בכיסאם תרמה לחידוד המודעות), היוו הפרסומים גם זרז לעשרות ומאות חברות סטארט אפ המציעות פתרונות טכנולוגיים לאיומים השונים.

מנהלי IT ומנהלי אבטחת מידע עומדים נבוכים אל מול שפע הטכנולוגיות, הכלים והפתרונות המוצעים להם. שאלת המפתח של רובם היא במה כדאי להשקיע ומה נחוץ פחות. במרוץ האינסופי בין תוקף למתגונן, החלטה שגוייה יכולה להיות הרת אסון למתגונן ולהפיל את מערך ההגנה. בשיחה שקיימתי לאחרונה, עם מנהל אבטחת מידע של מוסד פיננסי גדול, סיפר לי המנהל, כי ארגונו מפעיל מערך הגנה משולב של עשרות מוצרי אבטחה שונים. "איני רוצה לרכוש מוצרי אבטחה נוספים, בטרם אמצה את ההבטחה הגלומה בקיימים. גם כך, אנשי מתקשים לשלוט בכל הכלים הקיימים", אמר לי בן-שיחי. את האמירה המעניינת הזו, אפשר וצריך לפרק למספר שאלות משנה:
האם יש אמצעי שיאפשר למגינים למצות את ההשקעה שהשקיעו בכלים הרבים באופן טוב יותר? האם בכלל קיים נשק שובר שוויון בקרב בין התוקף למגינים? האם יש דרך למנוע את החדירה של "הרעים" לתשתית הארגון שלנו? אולי חשוב יותר להתמודד עם הנחת עבודה שהתוקף כבר פעיל בתוך הארגון? ואולי, ניתן להגביר את רמת ההגנה ולהפוך את מלאכת התקיפה ללא אפקטיבית?

התבוננות במידע שפורסם על מתקפות שונות, מעלה כי התוקפים פועלים בדרך דומה. לעיתים רחוקות עומד היעד תחת מתקפה ישירה. כמו בעולם הפיזי, יחפשו התוקפים נכס שמערך ההגנה עליו, מאפשר חדירה של מערך הביצורים. התוקף מצויד בד"כ בסבלנות רבה וההתקפות מנוהלות לאורך זמן ובעצימות נמוכה, העוברת בד"כ מתחת ל"מכ"ם" ההגנה של המגינים. בחלק מההתקפות שזכו לפרסום, הותקפו ספקי משנה של יעד התקיפה – כמו קבלני גיוס ומיון עובדים, ובחלק הותקפו עובדים דרך הרשתות החברתיות בהן היו פעילים. המשותף לשתי דרכי תקיפה אלה הוא רמת הגנה נמוכה, המאפיינת את מושאי ההתקפה הישירה. מרגע שהתוקף השיג אחיזה בגורם הראשון בשרשרת, מטרתו הבאה תהיה לנסות ולהשתמש בארכיטקטורת מערכות המידע והתשתיות של יעד המתקפה, לאיתור של חוליות טובות יותר. התנועה הרוחבית הזו ממשתמש למשתמש או משרת לשרת (lateral movement), מבוססת על הארכיטקטורה של ארגוני ה-IT, המאגדת נכסים דומים לאשכולות עליהם יופעלו אמצעי בידוד ואבטחה.
ארכיטקטורה זו מייצרת מקטעים שהכניסה אליהם מוגנת, אך מרגע שגורם עוין חודר לתוכם ,אין כל אמצעים למנוע את התנועה בין הפרטים במקטע (שרתים, תחנות עבודה וכדו'). התוקפים המודעים למורכבות ההגנה, ומבינים את ארכיטקטורת מערכות המידע של הארגון המותקף, ינצלו את מערך ההגנה ע"מ לשפר עמדות בדרכם אל היעד למתקפה.

ארכיטקטורה זו מייצרת מקטעים שהכניסה אליהם מוגנת, אך מרגע שגורם עוין חודר לתוכם ,אין כל אמצעים למנוע את התנועה בין הפרטים במקטע (שרתים, תחנות עבודה וכדו'). התוקפים המודעים למורכבות ההגנה, ומבינים את ארכיטקטורת מערכות המידע של הארגון המותקף, ינצלו את מערך ההגנה ע"מ לשפר עמדות בדרכם אל היעד למתקפה.

התנהלות זו של התוקפים, המבוססת על הארכיטקטורה, שבבסיס תשתיות הדטה סנטר (Data Center) שלנו, ועל המגבלות שלה, מזמינה חשיבה מחודשת על מבנה זה ועל דרכי ההגנה. אם נוכל לבודד באופן טוב יותר את המרכיבים השונים של המערכות שלנו, ולמנוע את התנועה הרוחבית, נקשה מאד על דרכם של התוקפים. בהשאלה מהעולם הפיזי, אם תקיפה של מרכיב אחד, לא מקנה לתוקף שלנו כל יתרון בתקיפת הרכיב הבא, הוא יאלץ לשקול מחדש את דרכו.

גישה זו, המכונה מיקרו סגמנטציה, מחלקת את הדטה סנטר למקטעים, שכל אחד מהם מייצג שלמות אפליקטיבית (למשל כלל מרכיבי מערכת ה-ERP) ומהווה מעיין דטה סנטר למערכת בודדת. באופן מפתיע, חלוקה זו, מפשטת גם את מדיניות האבטחה, שכן אין צורך להתחשב במערכות מקבילות, החולקות את אותם אמצעי הגנה ומקלה את ההגנה על המערכות. (חשבו למשל, מתי לאחרונה מחקתם חוק ב-Firewall? הסיבה שאיננו מוחקים חוקים, נעוצה בדיוק בשימוש המקביל של אמצעי האבטחה – ה-Firewall - על מספר מערכות מידע בו זמנית. או כפי שיאמר לכם איש אבטחה שלכם: "לכו תדעו על מי בדיוק משפיע החוק הזה").

עד לאחרונה, חייבה המיקרו סגמנטציה השקעה רבה בציוד אבטחה פיזי ולכן היתה יקרה מאד ולא מעשית בהיבט ניהול מערך האבטחה. הופעתם של פתרונות מתחום וירטואליזצית הרשת ואבטחת מידע, כדוגמת ה-NSX של חברת VMware מאפשרים מהפכה בארכיטקטורת האבטחה של הדטה סנטר.
כעת, ניתן לבנות ארכיטקטורה, שבבסיסה בידוד מוחלט של רכיבי מערכת אחת מיתר המערכות בדטה סנטר. אך לא די בכך. מדובר גם בשינוי בתפיסת ה"אמון" ברשת: מעבר מאמון גורף בין הרכיבים לבין הגדרה מפורשת של הרשאות גישה (Zero trust zone).

ארכיטקטורה חדשה זו, אינה רק בטוחה יותר בשל רמת הבידוד הייחודית שלה. מכיוון שהארכיטקטורה מבוססת על וירטואליזציה של מרכיבי התקשורת ואבטחת מידע, ניתן להוסיף באופן פשוט בכל שלב שירותי אבטחה נוספים (המשתלבים בווירטואליזציה). "הזרקת" השירותים מאפשרת התאמה של אמצעי האבטחה לאיומים, באופן פשוט יותר, מהמוכר לנו. זהו חלק מהמענה לצפייה של מנהל האבטחה עימו שוחחתי: לשפר וליעל השימוש בכלי האבטחה הקיימים. לסיכום, זהו עידן חדש בהתמודדות עם איומי אבטחת מידע וסייבר. עידן המבוסס כולו על וירטואליזציה של רשתות תקשורת ואבטחת המידע. הווירטואליזציה מאפשרת לנו לייצור אזורים, בהם פשוט להפעיל אמצעי הגנה ומניעה ולצמצם עד מאד יכולת התוקפים להגיע אל מידע רגיש. ארכיטקטורה זו הכרחית בעידן שבו איומי הסייבר מאיימים להטביע את ספינות ה-IT שלנו והיא מאפשרת להציב מענה הולם לאתגרי הסייבר. עשרות רבות של לקוחות ישראליים, כבר ממשים פתרון כזה ברשתות שלהם. האחרים מוזמנים להתנסות.
כפי שאמר העתידן והסופר ויליאם גיבסון: "The future is already here — it's just not very evenly distributed."

מאת: אילן ינובסקי | אסטרטג פתרונות עסקיים אזורי VMware

