צילום: shutterstock

כי בתחבולות תעשה מגננה

בדומה לעולם הביון, גם במרחב הקיברנטי יש לנקוט בגישת ההגנה האקטיבית כדי להשיג יתרון בזירת לוחמת הסייבר

מאת ד"ר גיל דוד

ערכות ההגנה מפני התקפות סייבר על מחשבים ורשתות מבוססות רובן ככולן על הגנה פאסיבית. מערכות אלו משתמשות במנגנונים ושיטות לזיהוי פעילות פוגענית והתקפות כגון וירוסים, סוסים טרויאנים, תולעים ועוד. השיטות הן בדרך כלל פאסיביות, כלומר, מערכות ההגנה בוחנות את הפעילות התקשורתית ברשת המקומית או במחשב ומנסות לזהות את התקיפה ללא התערבות בפעילותו של התוקף או של כלי התקיפה. בעת גילוי הפעילות הזדונית, מערכות אלה יכולות לעבור לשלב האקטיבי בו הן חוסמות את התוקף או משמידות את כלי התקיפה (למשל, הוירוס). מעבר לכך, המערכות הפאסיביות הן בדרך כלל במצב תמידי של מגננה. הן לא יודעות מהיכן תגיע ההתקפה ובאיזה צורה אבל הן יודעות שבסוף היא תגיע – הן יושבות במחפורת ומחכות לבואה ומקוות שהן יצליחו לזהות אותה בזמן לפני שהיא מצליחה לחדור את קווי ההגנה הוירטואלים.

התפיסה המקובלת מאז ומעולם בעולם הסייבר הינה, שמטרת אמצעי ההגנה היא לזהות ולחסום את התוקף מהר ככל האפשר ולהפסיק את פעילותו הזדונית בהקדם האפשרי. התקווה של מערכות ההגנה היא שאפילו אם וירוס מתוחכם או תולעת חדשנית יצליחו לחדור, די מהר יתגלו עדויות לתקיפה וניתן יהיה לעדכן את אמצעי ההגנה כך שיוכלו לחסום אותם.

לאסטרטגיית הגנה זו יש מספר חסרונות עיקריים. מצד אחד, המגן מוגבל מבחינת יכולת הזיהוי הפאסיבית שלו ותמיד יהיו כלי תקיפה חדשים יותר שיידעו לחלוף על פניו. כלומר, המגן יודע להגן רק מפני מה שהוא מכיר או יודע לזהות באמצעות כליו. מצד שני, בעת גילויו של התוקף או כלי התקיפה, המגן חוסם אותו ואף משמידו במידת האפשר. בפעולה זאת, המגן מאבד מידע מודיעיני רב ערך שעשוי היה להועיל לו רבות לשם שיפור מערך ההגנה שלו ואף מעבר לכך.

במאמר זה נציג גישה שונה לאסטרטגיית ההגנה המקובלת. גישה זו משלבת אלמנטים של הגנה אקטיבית, בה המגן עובר ממצב פאסיבי של המתנה לתוקף (מתוך תקווה שלא יגיע) למצב אקטיבי בו המגן מחכה בקוצר רוח לתוקף ומשלב שיטות, שרווקא יגרמו לתוקף לבצע את התקיפה.

לשם ההמחשה, בואו נסתכל על דוגמא בידיונית מעולם הביון. נניח שמדינה מסויימת מגלה שיש מרגל שהושתל במתקן רגיש כגון כור גרעיני. על פי אסטרטגיית ההגנה הפאסיבית, הגוף המגן מבצע תחקירים ביטחוניים לעובדיו וניטור של פעילותם על מנת לזהות גורמים עוינים בתוך האירגון. בהנחה שפעילות המרגל עוררה חשד והוא זוהה על ידי המגן, מיד עם חשיפתו של המרגל, על פי ההגנה הפאסיבית הוא יחוסל. ברור שעם חיסולו תיפסק פעולת הריגול אותה הוא ביצע אך ברור עוד יותר שעם חיסולו מאבד המגן מידע חיוני כגון עבור מי הוא עבד, מה הנזק שהוא גרם לו עד כה, מה כוונות מפעיליו לעתיד וכו'. בנוסף, ייתכן שמרגל חי עדיף על מרגל מת וניתן היה להשתמש בו נגד מפעיליו.

לפי אסטרטגיית ההגנה האקטיבית, המגן לא מחפש את המרגל על ידי ניטור של פעילות עובדיו וחיפוש מאפיינים חריגים אלא הוא מנסה להערים על המרגל על מנת שזה יבצע טעות ויחשוף את עצמו. כלומר, המגן מטמין מלכודות ומנסה למשוך את המרגל על מנת שיפול באחת מהן. למשל, המגן יכול להשאיר את הדלת לאחד החדרים הרגישים ביותר בכור פתוחה במתכוון ולבצע מעקב סמוי אחר הנכנסים מתוך כוונה שאחד האנשים הבלתי מורשים שיימשכו למלכודת וייכנסו לאזור הרגיש הינו מרגל. עם נפילתו של המרגל למלכודת וחשיפתו, המגן עובר לשלב הבא בו הוא מבצע מעקב רצוף אחר פעולותיו, ללא ידיעתו של המרגל. כלומר, המגן יודע מיהו המרגל אך הוא לא עוצר אותו או מפסיק את פעילותו. באופן זה, המגן יכול לדעת מהן כוונותיו של המרגל, איזה מידע הוא אוסף, מהן שיטות הפעולה שלו, מיהם מפעיליו, האם ישנם מרגלים אחרים עימם הוא נמצא בקשר וכו'. מדובר במידע שערכו לא יסולא בפז ולמעשה הוא מאפשר לתוקף ללמוד בצורה הטובה ביותר את שיטות הפעולה של המרגל ואת הנזק אותו הוא גרם. בשלב האחרון של ההגנה האקטיבית, המגן מבצע "הכפלה" של המרגל ללא ידיעתו. כלומר, המגן מאפשר למרגל להמשיך את פעולת הריגול אך המידע אותו גונב המרגל ומעביר למפעיליו איננו המידע האמיתי שקיים במתקן אלא כל מידע בדוי או מוטה אותו רוצה המגן להעביר למפעילי התוקף. למשל, המגן יכול להטעות בדרך זו את מפעילי המרגל כך שיחשבו שמועד הפיכתו של הכור הגרעיני למבצעי הינו רחוק במספר שנים מהמועד האמיתי.

כפי שניתן לראות, ההגנה האקטיבית הופכת בשלב מסויימת לסוג של התקפה כנגד התוקף המקורי אפילו מבלי שהתוקף מודע לכך שהוא נמצא תחת מתקפה.

הגנה אקטיבית בעולם הסייבר

באופן דומה לעולם הביון, גם בעולם הסייבר אנו עוסקים במרגלים וכלי ריגול למיניהם כגון

אילוסטרציה: shutterstock

"לגישה של הגנה אקטיבית, ישנם יתרונות רבים, והיא יכולה להוות מצד אחד כלי משלים לגישת ההגנה המסורתית, אך מצד שני היא יכולה גם להפוך את תמונת הקרב על פיה ולהכריע את הכף במלחמות הסייבר הקרבות ובאות"

תולעים, וירוסים וסוסים טרויאנים. גם כאן, הכלים הפוגעניים מבצעים מגוון פעולות ריגול. החל מאיסוף מידע רגיש, דרך לימוד הרשת כשלב מקדים לתקיפה עתידית ועד לביצוע פעולות הרסניות כגון השבתת צנטריפוגות וכיבוי מתקנים אסטרטגיים.

כיצד ניתן ליישם הגנה אקטיבית בעולם הסייבר? לצורך כך יש לשנות גישה ולתקוף את הבעיה מכיוון שונה לחלוטין בו נוקטת אסטרטגיית ההגנה הפאסיבית. לפי ההגנה האקטיבית, המגן יוזם פעולות אקטיביות שמטרתן הינה למשוך אליו את התוקף ולגרום לו לבצע את התקיפה בתנאים אותם מגדיר המגן ובסביבה הנוחה לו. המגן למעשה מייצר עבור התוקף פרצות באופן מכוון כדי למשוך אליהן את התוקף. מכיוון שהמגן מודע לפרצות האלה שכן הוא יצר אותן, הוא יכול לנטר אותן ולזהות מתי כלי מסויים מנסה לחדור דרכן. למשל, המגן יכול להשאיר פתוח שירות (port) מסויים במחשב ולאפשר לכל אחד לחדור דרכו. בדומה לדוגמא של המרגל והדלת שהושארה פתוחה, המגן מטמין לתוקף מלכודת ומקווה למשוך אותו בדרך זו וכך גם לחשוף אותו. מלכודות אלא נקראות בעולם הסייבר HoneyPots, מלכודות דבש. המגן יכול לייצר רשת שלמה של מלכודות דבש ובאופן הזה לדמות רשת שלמה באירגון ולא רק מחשב יחיד. רשת כזה מכונה HoneyNet, רשת דבש.

בדרך כלל, המלכודות יוטמנו באיזור נפרד מהרשת האמיתית של האירגון על מנת לצמצם את הנזק במידה והתוקף יחדור פנימה וינסה לפגוע ברשת האמיתית. למעשה, המגן מייצר עבור התוקף עולם וירטואלי המכיל רשתות, מחשבים ומשתמשים וירטואלים שכל מטרתו היא למשוך אליו את התוקף ולגרום לו ליפול למלכודת ולהיכנס לעולם מקביל זה ולא לרשת האמיתית של האירגון. עולם זה לא מכיל את המידע הרגיש הנמצא באירגון וכל פעילות פוגענית בו לא יכולה להשפיע על הרשת האמיתית של הארגון ולכן לא יכולה לפגוע בצד המגן בשום אופן.

בדרך זו המגן יכול לזהות ולחשוף את התוקף ללא שימוש באמצעי ההגנה המסורתיים (כגון אנטי-וירוס, חומות אש וכו') אלא חשיפתו תתבצע עקב נפילתו למלכודת. אולם מעבר לגילויו של התוקף, השימוש במלכודות המייצרות פרצות עבור התוקף גורם לו לנסות לחדור אל האזור הפרוץ יותר, אליו קל לו לחדור (פירצה קוראת לגנב), ולא לאזור המוגן יותר, כגון הרשת האמיתית של הארגון. כתוצאה מכך, העולם הוירטואלי רווי המלכודות המפתות שיוצר עבור התוקף ירחיק אותו ללא ידיעתו מהרשת האמיתית ולמעשה יחזק באופן ניכר את מערך ההגנה המסורתי.

לאחר חשיפתו של הכלי הפוגעני, יכול המגן לעבור לשלב הבא בו הוא לומד את דרכי הפעולה של התוקף, דרכי ההתקשרות של הכלי התוקף עם מפעיליו המרוחקים (ובדרך זו הוא יכול לזהות את שרתי השליטה והפיקוד איתם הוא מתקשר), הדרכים בהם הוא משתמש להזליג מידע רגיש מחוץ לארגון, מהות המידע אותו הוא אוסף ומטרתו (למשל, מיפוי הרשת כשלב מקדים לתקיפה), האיזורים בתוך הארגון בהם הוא מתעניין (למשל, מסמכים מסויימים המאוחסנים בשרת קבצים מסויים), דרכי ההתפשטות שלו וההדבקה של מחשבים אחרים וכו'.

כתוצאה מכך, המגן יכול לבנות תמונה מודיעינית שלמה על התוקף ולאפיין את דרכי פעילותו באופן מדוייק. מהצד ההגנתי, המגן יכול להשתמש בנתונים אותם הוא אסף לגבי התוקף על מנת לזהות כלי תקיפה אחרים בעלי מאפיינים דומים. מהצד ההתקפתי, המגן יכול ללמוד דרכי תקיפה חדשות ולהשתמש בהן לצרכיו ובכך לשפר את מערך התקיפה שלו.

בשלב האחרון של ההגנה האקטיבית, שלב "הכפלת" הכלי התוקף, המגן יכול ליצור עבור התוקף עולם תוכן שלם כרצונו. כלומר, המגן יכול לשתול ברשת הדבש הוירטואלית מסמכים בדויים כראות עיניו כך שהכלי התוקף יעבירם למפעיליו שיאמינו שמדובר במידע מהימן המגיע מרשת רגישה. למשל, המגן יכול לגרום לתוקפים לחשוב שתאריך הפיכתו של הכור למבצעי הינו רחוק במספר שנים מהמועד האמיתי. בנוסף, המגן יכול לגרום לתוקף להאמין שכל המחשבים בארגון מודבקים בכלי הפוגעני וביום פקודה התוקף יוכל להשבית את המערכות ולגרום לנזק משמעותי. בפועל, מכיוון שמדובר בעולם וירטואלי שנוצר עבור התוקף, ולא ברשת האמיתית של הארגון, כאשר תתקבל פקודת התקיפה ביום הדין, תמשיך הרשת האמיתית לעבוד כסידרה שכן הפעילות הזדונית תישאר כלואה בעולם הוירטואלי.

לגישה זו, של הגנה אקטיבית, ישנם יתרונות רבים, והיא יכולה להוות מצד אחד כלי משלים לגישת ההגנה המסורתית, אך מצד שני היא יכולה גם להפוך את תמונת הקרב על פיה ולהכריע את הכף במלחמות הסייבר הקרבות ובאות. אסטרטגיית ההגנה האקטיבית משלבת אלמנטים חדשניים ולא שיגרתיים שבאופן עקיף גם יכולים לשפר באופן ניכר את מערך התקיפה של הגוף המגן וכך להילחם בתוקף בשיטותיו הוא ולפנות את כלי התקיפה שלו כנגדו.

בעזרת אסטרטגיית ההגנה האקטיבית יכול המגן להפוך התקפות סייבר משמעותיות ביותר לאיום ממשי דווקא על הצד התוקף כך שההתקפה תהיה למעשה חרב פיפיות עבור הצד התוקף. שילובן של שיטות אלה במערך ההגנה יכול להוות תשובה הולמת להתקפות להם אנו עדים לאחרונה ולחזק באופן ניכר הן את מערך ההגנה והן את מערך ההתקפה.

ד"ר גיל דוד הוא הבעלים והמנכ"ל של חברת Brainstorm Private Consulting לייעוץ בעולם הסייבר והמודיעין. הוא משמש כפרופסור אורח באוניברסיטה באירופה ומשתף פעולה עם גופים ביטחוניים, מסחריים ואקדמיים בארץ ובעולם.