

במהלך נאומו תיאר דוקט את מה שקורה בעת שמבוצעת חדירה למערכת על ידי רושעה או נזקה כלשהי, כזו שמטרתה לגרום נזק בדמות פעולה שמבוצעת במחשבי החברה. "כל חדירה למערכת מורכבת משלושה שלבים מובהקים", הוא הסביר. "השלב הראשון הוא הכניסה בצורה הכי פשוטה לתוך המערכת. זה יכול לקרות כתמונה שנשלחת לדואר, שמישהו בארגון בסופו של דבר עושה עליה לחיצה כפולה מבלי לחשוב, וכמעט תמיד ייצא מי שיעשה זאת. השלב השני הוא תנועה לישראלית של הקובץ המזיק, שמטרתו לזהות מידע רב ערך וחומרים שהם רכוש חשוב, כמו קניין רוחני. הצעד השלישי הוא לבצע את הפעולה עצמה, את העברת המידע, הקבצים, יצירת הנזק עצמו".

וכאילו להגדיל את המשמעות של הנזקים שיכולים להתרחש כיום, טען דוקט שלא משנה מה עושים כולם, ועד כמה מתגוננים בסופו של דבר כל ארגון יסבול מחדירה, ולא משנה "זה אומר שצריך להתכונן למקרים בהם כבר יש חדירה ופיגוע במערכת הכוללת, לספק הגדרות שמונעות פעילות בתוך המערכת גם אם הנוזקה עברה את הקווים הראשונים, וזאת תוך כדי שצריך להבין דבר אחד מאוד פשוט: שלא יהיו סיפורים ואגדות, כל רושעה היא קובץ. נקודה. את הקובץ הזה צריך לאתר", הוא הסביר.

כדי להראות את היכולות של הטכניות של פתרון הפירוול שמציעה פאלו-אלטו סיפק דוקט הדגמה חיה של המערכת, תוך שימוש במכונה חיה. הוא הדגיש שנקודת ההשקפה של החברה, והיתרון של פתרון הפירוול שלה, היא ההתמקדות באפליקציות ובקבצים במערכת ולא בפורטים, תוך בדיקת כל היכולות באמצעות חוקה אחת שמוגדרת במקום אחת עבור כל מחלקות הארגון.

"אי אפשר להתעלם מההקשר של מיקום הקבצים והאפליקציות"

חוזת מוניס, מהנדס מכירות של פאלו אלטו באזור איטליה, התייחס גם הוא ליכולות פתרון הפירוול שמציעה החברה. "אי אפשר לקחת כיום פתרון הגנה ולהתקין אותו מבלי להתייחס להקשר שלו בסביבת העבודה", הוא אמר. "אבל מה זה הקשר? ולמה הוא בכלל חשוב? כי אם לא עושים את ההקשר הנכון אז אי אפשר ליישם פתרון אינטליגנטי, ואם אין לכם פתרון אינטליגנטי, אתם גם לא יכולים לספק מענה אבטחה אינטליגנטי לבעיות שאתם צריכים להתמודד עמן".

לטענתו, בדיקת ההקשר של האבטחה משנה לפעמים את התמונה מקצה לקצה, במיוחד לגבי הצרכים ולגבי הפתרון שבו בוחרים בסופו של דבר. "כך לדוגמה, אי אפשר להתעלם מההקשר של מיקום הקבצים והאפליקציות. אם חלקים גדולים של העבודה שלכם ממוקמים כיום



בן כפולר

בן כפולר: "ההאקרים הרבה יותר מתקדמים ממה שנוטים לחשוב. אלה כבר לא האקרים 'קטנים' אלא ארגונים שמושקעים בהם הרבה מאוד משאבים ומוטיבציה"



רוני דוקט



חוזת מוניס

מולם. צריכים להבין שלא ניתן למנוע את המתקפות לחלוטין ומכיוון שכך, המטרה היא לנסות כל הזמן להעלות את הרף, כדי להתמודד עם האיומים הללו. לנסות כל הזמן לבנות מכשול עוד יותר קשה בפני התוקפים, בדרכים שהם לא ממש יכולים לצפות להן, כאלה שמקשות עליהם יותר ויותר לאסוף את המשאבים שדרושים למתקפה מוצלחת".

הוא ציין כי אין כיום תשובה חד משמעית האם המנצחים במערכה הם ההאקרים או אלה שמתגוננים מפניהם, בין היתר מאחר ש-"כבר לא ברור בדיוק מהי ההגדרה הנכונה להצלחה, האם היא זהה למה שהייתה פעם".

כפולר הוסיף שיש לקחת בחשבון את השינוי באופן ובמקום השימוש בפלטפורמות המיחשוב הארגוניות. "מפת השימושים כיום שונה מאוד מזו שהכרנו עד ממש לאחרונה. זה כבר לא רק במשרד, מדובר באפליקציות ובשימושים של לקוחות שרבים מאוד מהם שימושים מרוחקים. גם התשתית כבר לא תמיד יושבת בחדר המחשב בבניין הראשי של הארגון שלכם. השינוי הזה יוצר הזדמנות גדולה מאוד למי שרוצה לתקוף את הארגון".

לעומת זאת, לדברי כפולר, תקני האבטחה איבדו מחשיבותם. "לפעמים, הנושא הזה לא רלוונטי לחלוטין. ברגע שמתגלה פרצה המידע כבר יצא, כך שהתיקון לבדו לא יעזור. בפעם הבאה שהארגון יותקף על ידי האקר שמצא את הפרצה במערך ההגנה שלו, הוא לא יחזור להשתמש באותה תקיפה אלא יחפש חור אחר, חדש לחלוטין", אמר.

כפולר תיאר שלושה אלמנטים קריטיים ליכולת של הארגון להגן על עצמו: איתור וזיהוי התקיפה, יכולת להגן עד ליצירת התיקון והאלמנט החשוב ביותר לטענתו - שימוש בפלטפורמה שיוודעת לבצע את המניעה הן בצד של הרשת והן בנקודות הקצה. "יש צורך בפלטפורמה שמטפלת במה שמדאיג אותנו, וזה לא מה שאנחנו מכירים אלא מה שאנחנו לא מכירים, בכל תצורות הרשת האפשרויות. פאלו אלטו נותנת את הפתרון הטוב ביותר בנקודות הקצה, והיא יכולה כל הזמן, תוך כדי תנועה, לשפר את רמת האבטחה הן ברשת והן בנקודות הקצה", טען כפולר.

כל האיומים השתנו

"בסופו של דבר, הרי הפירוול הוא סוג של מסננת. זה אומר שאם אנחנו לא נגדיר אותה היטב, בצורה הנכונה, אז אנחנו בעצם ניצור חורים שפשוט יעבירו את מה שאנחנו למעשה מפתחים ממנו. ולמה צריכים לדבר על זה, מה השתנה? כי כפי כבר שאמרנו לא אחת,

כל האיומים השתנו. המטרה שלהם היא לגנוב כסף או מידע, ובמקרים מסוימים אף לשנות את המידע ששומר במחסנים שלנו, אם יש בכך ערך לטווח ארוך", אמר רוני דוקט, מהנדס מכירות בכיר בפאלו-אלטו נטוורקס.