פתרונות מבוססי ענן, שמהווים "סיירת סייבר" עבור הארגון. בעזרת צוותים מיומנים ופתרונות טכנולוגיים מציעה החברה התראות על סכנות מהתקפות על אפליקציות בתחום המסחר האלקטרוני, שירותים פיננסים, בריאות ועוד.

"אנחנו מאמינים שטכנולוגיה לבד לא יכולה לעשות את העבודה אלא בשילוב עם אנשים. אנחנו מגדירים את עצמו כסיירת הביטחון של האתר שלכם השומרת עליכם 24 שעות וצופה בכם כל הזמן. החברה מפעילה שיטת BI מודיעין עסקי וכן פעילות ברשת החברתית כדי לאתר איומים וסכנות שמופנות כלפי הארגונים מצד האתר שלהם, ואף מציעה פתרונות מקצה לקצה אבטחת אתרים, מבוססי שירותי ענן", סיכם את דבריו.

"אנחנו עובדים בעסק של הפחדות"

"אנחנו עובדים בעסק של הפחדות. כל היום אנו סורקים את האיומים ובכנס הזה הפחדנו אחד את השני היטב", אמר **צורי תמם**, מהנדס פריסייל בכיר ב-F5, והוסיף כי "הסיבה היא שמרחב האיומים חצה מזמן את גבולות הרשת. ארגונים נעשו הרבה יותר מבוזרים, ולמעשה מבחינת איומים אנחנו מדברים על ארגונים ללא גבולות".

"להאקרים יש מגוון שיטות של הפצצות על אתרים במטרה להשבית שירותים חיוניים ולפגוע במהלך החיים התקין. ה-DDOS שכולם מדברים עליו כעת, הוא בעצם מסך עשן שהאקרים משתמשים בו על מנת לשים יד על מידע רגיש, שבסופו של דבר ייצר גניבת כסף או גניבת מידע לצרכים פוליטיים", הסביר תמם.

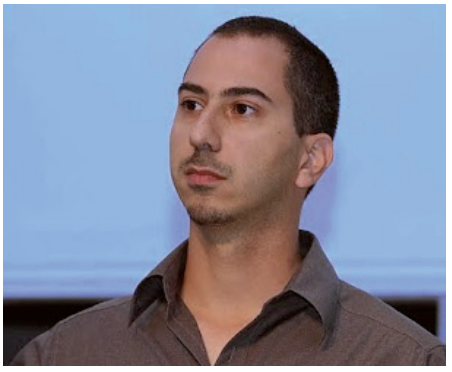
תמם הוסיף וסיפר, כי "ב-F5 רואים את התשתיות כיעד מרכזי להתקפות ולכן פיתחנו מערכות שיודעות לזהות התקפות על תשתיות, אחרי שסיננו את הרעש ואנו מבינים שמי שעשה את הרעש מחפש לבצע נזקים אפליקטיביים".

בין היתר הציג את פתרונות Web Safe של F5, עליהם אמר כי "מדובר בסוויטה של מוצרים שיודעת להגן על הארגון בכל שלבי התהליכים מהרגע שהמשתמש נכנס לאתר, מפעיל אפליקציה ומייצר טרנזקציות".

"ההאקרים לא עובדים כל כך קשה"

עדי פרץ, אנליסט אבטחת מידע ב-Cyber Trust, הסביר על כך ש-"האתרים והחברות מהווים סביבה חשופה להתקפות, שמגיעות בגלל רצון הארגונים להיות מחוברים ולהעניק כמה שיותר שירותים ללקוחותיהם. כמויות המידע הן עצומות וההאקרים פועלים מתחת לרדאר".

"ההאקרים לא עובדים כל כך קשה כמו שאתם חושבים השיטות שלהם פשוטות יחסית, למשל דרך צירוף קורות חיים למייל. זה הדבר שאנשים הכי הרבה פותחים. ברגע שהמשתמש פותח את הקו"ח ההאקרים עולים על הלוגים שלו ומרגע זה הוא במעקב מתמיד, הסביר פרץ".



צורי תמם

משה זריהן

ירון מזור

הפתרון צריך להיות משולב טכנולוגיות ואנשים. אסור לבחור בפתרונות של שיטת הדייג, אלא להיות מאוד ממוקדים כי מספיק שפעם אחת הם מצליחים. לכן יש לשלב טכנולוגיה ואנשים שיודעים לנתח תהליכים להפיק לקחים ולמזער נזקים.

"בסך הכל אנליסט אבטחת מידע צריך לדעת לנהל סיכונים, להיות בעל יכולת חשיבה אנליטית, יכולת יחסי אנוש, כושר כתיבה, ניהול תהליכים ותקשורת בינאישית. כלומר, אנליסט חייב לייצר גישה אקטיבית ללוחמת סייבר ולא רק להתגונן", אמר פרץ.

"לשדרג את הרמה של לוחמי אבטחת המידע"

"כל הארגונים, קטנים כגדולים, חייבים לשדרג את הרמה המקצועית של הצוותים המתמודדים עם אירועי אבטחת המידע. ארגון שרוצה לשמור על המערכות שלו צריך לשאול את עצמו האם הצוות והמשאבים שהוא יכול להצמיד לאתגרים יכולים לעמוד בהם", כך אמר **משה זריהן**, סמנכ"ל הטכנולוגיות של חברת Thrustnet. לדבריו, "אין כיום משמעות לגודל החברה. כל חברה היא יעד למתקפה".

בדבריו מנה זריהן את הכישורים נדרשים ללוחמי סייבר, אנשי אבטחת מידע ומומחי אבטחה בצוות CERT. "עליהם להבין היטב בתקשורת, כדי לנסות לזהות חריגות. הם גם חייבים להבין משהו בסיסטם, כי במקרה של פופ אפ 'תמים' לכאורה שקפץ אצל אחד העובדים, עליו לזהות שמדובר בהתראת פריצה. תחומים נוספים בהם הוא חייב להבין הם מודיעין - טכנולוגי ולא טכנולוגי - וקוד, כדי לבצע ניתוח והנדסה לאחור של קוד שהמערכת מגלה ושלחברות האנטי וירוס אין עדיין חתימה שלו".

"עליו להיות בעל הבנה באבטחת מידע ויכולת ראייה מרחבית, ולהבין מהו התחום העסקי של הארגון", הוסיף זריהן. "קשה למצוא אנשים שיש להם את הידע המעמיק הזה. צריך לשאוף להקפיץ את כולנו לשם".

הוא אמר כי "ניתן לעשות זאת באמצעות שימוש במשאבים פנימיים - דבר שמחייב לשדרג את צוות התגובה, או באמצעות חברות חיצוניות, בכפוף לאפשרות הרגולטורית. בנוסף, יש כיום שירותי CERT בענן, שגם השימוש בהם כפוף לאישורים הרגולטוריים בענף שבו פועל הארגון".

לדבריו, "יש כיום שירותים רבים המזהים האקרים מוכרים וטכנולוגיות, כמו SandBox, שמריצים את הקובץ באזור מוגן כדי לאתר קוד עוין. השאלה היא האם לאחר התקנת השירותים הללו, יש מי שיידע להפיק את התועלות מהמערכות המתוחכמות".

זהירות - משתמשים פריבילגיים

ירון מזור, מנהל פרויקטים אסטרטגיים בישראל ובמזרח אירופה ב-CyberArk, הזהיר מפני משתמשים שיש להם רשות להיכנס לכל מערכות התוכנה ואמר כי "הם יעד לתוקפים, וכאשר תוקף נכנס בסיסמה של משתמש כזה קשה מאוד לעצור אותו".