

שיודעים לזהות את המשתמש ולהעניק לו הרשאות גישה מוגבלות וממוקדות למידע".

ד"ר ווינטר סיים בצינון ש-HP מספקת פתרונות מקצה לקצה לאבטחה חכמה ולבקרת גישה של משתמשים בעלי זכויות יתר, כחלק מפלטפורמת Security Intelligence Platform. פתרונות האבטחה מאפשרים לארגונים להמשיך ולהתקדם לקראת הפיכתם לארגונים שיודעים להגיב באופן מיידי, עם יכולת תגובה מהירה יותר לשינויים, דרישות והזדמנויות".

"לטפל באיום כשהוא 'מחוץ לגדר'"

"היעד אליו נדרשים ארגונים להגיע הוא לטפל באיום מבעוד מועד, כשהוא טרם הגיע לארגון, נמצא 'מחוץ לגדר', כך אמר **רוני בלוק**, CTO קבוצת אמן.

לדברי בלוק, ארגונים אזרחיים נדרשים לטפל באיומים המתקרבים באמצעות מתודולוגיות צבאיות. "במגזר הציבורי קיימים מזה שנים גופים מוסדרים שחוקרים את נושאי הסייבר. המגזר הפרטי מתחיל לעשות זאת כעת, כי חברות מבינות שעל מנת להגן על הנכסים שלהן צריך להבין את האיומים, ומהר", אמר.

הוא ציין, כי "פעילות קיברנטיקה יכולה לפגוע בעסקים ולגרום לרדף מסחרי או אישי, שיבוש מידע, שיתוק מערכות וניצול מערכות אבטחה".

"האם סטוקסנט או דומותיה יכולות לפגוע בארגון שלי?", שאל בלוק שאלה רטורית, והשיב: "חדרי מחשב עם מערכת הגנת טמפרטורה יכולים להיות משובשים. גם שיבושים טכנולוגיים אחרים, שאינם וירוסים, עלולים לפגוע במתקנים באופן שיעבור זמן רב עד מציאת



רוני בלוק



ד"ר פרסקוט ווינטר

מקור התקלה".

"אחד הדברים שאנחנו צריכים לעשות עם 'לוחמה מחוץ לגדר' הוא לטפל באיום לא רק כאשר הוא מגיע אלינו לארגון אלא מבעוד מועד - מחוץ לגדר", אמר בלוק. "כאן ניתן ללמוד כיצד פועלים הארגונים הביטחוניים-לאומיים, על כך שהם עובדים בשלושה מישורים - הגנת, מודיעיני (בתוך הארגון ומחוצה לו) והתקפי - ועל כך שהם עושים זאת לאורך זמן. השלכת המתודולוגיה הזו על גופים פרטיים היא חלק מהגישה של אמן להתמודדות המגזר הפרטי עם מפת האיומים החדשה". בלוק הוסיף, כי "יש לבצע ניתוח אסטרטגי, לאסוף מידע מחיישנים מודיעיניים ולאחר מכן לעבור לכיוון התקפה. לא ניתן לתקוף כל אחד, אפילו אם אנחנו יודעים שהוא הולך לתקוף אותנו".

"הגופים הביטחוניים מקבלים מידע ממערכות השליטה והבקרה (שו"ב) והחיישנים הפרוסים בשטח ומנהלים את המלחמה כמה שיותר רחוק, באופן שוטף ועם מודיעין מדויק ככל שניתן", ציין. "להבדיל מהשדה הצבאי, בשוק הפרטי יש מגבלות רגולטוריות ובנוסף, ארגונים לא יכולים להרשות לעצמם להתנתק מהאינטרנט".

עוד אמר בלוק, כי "רוב המתקפות הן על כמה גופים בו זמנית. למשל, בתקיפה על ארגון במערכת הבריאות, גידול בזימון תורים יכול להיות תמים - כגון במקרה של תחלואה עונתית, אך הוא יכול להיות אירוע סייבר. חייבים לזהות מהר את האנומליות. אנחנו רוצים להפעיל הרבה חיישנים טכנולוגיים ברשת וכל המידע צריך להיכנס למערכת השו"ב, תוך הכללת המידע והתכתו לאנליסטים. מתוך המידע הזה הם יבינו שמתחוללת התקפה ושיש להתגונן בהתאם".

"מערכת השו"ב", הדגיש בלוק, "היא לב העניין. אנחנו רוצים לקבל תמונת מצב עדכנית ולשם כך צריך לשתף פעולה עם ארגונים אחרים

באמצעי התקשורת ולא על התקפות אחרות שאינן נוגעות לאתרים ציבוריים. לדעתי אנו רואים רק את ההתחלה וזה לא יפתיע אותי אם במקביל להתקפות DDoS (מניעת שירות מבוזרת) כאלה ואחרות, יתנהלו מתקפות מזיקות בהרבה, אשר הציבור טרם נחשף אליהן".

הוא סיכם באומרו, כי "ההאקרים נעשים יותר מתוחכמים והמתקפות נגד אתרים וגופים ישראליים רק ילכו ויתגברו. יש להתייחס לעניין ככובד ראש ולהכין עצמנו לקראת מתקפות נוספות".

"כל המידע הארגוני מצוי תחת מתקפה"

"הנחת העבודה שארגונים נדרשים לעבוד על פיה היא שכל המידע שברשותם מצוי תחת שרשרת בלתי פוסקת של מתקפות. אל לכם, מנמ"רים ומנהלי אבטחת מידע, לחשוב ולו לרגע שאתם מוגנים. אם תעשו זאת - אתם טועים ומטעים", כך אמר ד"ר **פרסקוט ווינטר**, CTO בחטיבת האבטחה הארגונית למגזר הציבורי ב-HP העולמית.

לדברי ד"ר ווינטר, "המתקפות אינן מבדילות בין סוגי המידע. מידע מובנה ובלתי מובנה, מסווג ובלתי מסווג, קניין רוחני ומידע אישי - הכול פגיע". "היבט נוסף הכרך במתקפות הוא שאין להעריך את הנזק הבל יסוער עקב אובדן המידע או גניבתו, אלא להניח שהנזק מצוי במגמת עלייה. ארגונים מצויים כיום בחזית המתקפות", אמר. "מגמה המסייעת למתקפות היא השיתופיות - זו שבתוך הארגונים וזו שבין הארגון ללקוחות ולשותפים העסקיים שמחוצה לו. הכול רוצים את המידע הארגוני, ולכן - אי אפשר לסגור את המידע באופן הרמטי". "יש להתעסק עם אותם סיכונים, לבחון ולמפות אותם.

אין פתרון נקודתי", אמר הבכיר ב-HP. הוא ציין, כי "אנחנו בונים רכיבי אבטחת מידע ותוכנות לתחום. העניין אינו נוגע למערכת אחת, אלא נדרשת סביבה כוללת בנויה באופן מאובטח מההתחלה". ד"ר ווינטר אמר שתפיסת אבטחת המידע הכוללת שעל ארגונים לנקוט מורכבת מאסטרטגיה, ממשל, תפעול ומפעילים, מסגרות עבודה והגנת הליבה העסקית.

הוא ציטט נתונים ממחקר שערך מכון פונימון, במימון HP, שמצביע על סיכון הולך וגובר לחשיפת נתונים רגישים או חסויים. זאת, כתוצאה מהיעדר בקרה ופיקוח על משתמשים בעלי זכויות גישה נרחבות, ובהם מנהלי בסיסי נתונים (DBA), מהנדסי תקשורת ואנשי אבטחת מידע בארגונים. מהמחקר עולה, כי יותר ממחצית מעובדי הארגונים יכולים לגשת למידע סודי באופן החורג מדרישות התפקיד שלהם. נתון בעייתי נוסף אותו ציין ד"ר ווינטר הוא ש-64% מעובדי הארגונים מסרו שהם ניגשים לפריטי מידע חסויים או רגישים מתוך סקרנות בלבד ולא רק עקב צורך עסקי. "מידע אודות לקוחות ומידע עסקי כללי נמצאים בסיכון גבוה במיוחד, כאשר נקודות החשיפה העיקריות הן יישומים ייעודיים לחטיבות עסקיות, יישומי רשתות חברתיות ויישומים ניידים", אמר.

"פתרון SIEM - קריטי לאבטחה"

"הטמעת פתרון לניהול מידע ואירועי אבטחה (SIEM) הינה צעד קריטי בדרך ליצירת גמת אבטחה גבוהה יותר", ציין ד"ר ווינטר. הוא הוסיף, כי "קיימים סיכונים שארגונים אינם ערים להם ואינם עומדים בשורה אחת עם התקנת טלאי אבטחה, יצירת מערכי הגנה היקפיים וסוגיות נפוצות אחרות בעולם האבטחה. ארגונים נדרשים לניהול טוב יותר של מדיניות הגישה בארגונים, כמו גם לפתרונות חכמים ומתקדמים יותר, כאלה