לתפוס את אתי אלון הבאה בזמן הסטארט־אפ הישראלי שיחשוף עובדים סוררים לפני ביצוע עבירה אמיתי זיו 10

TheMarker

הסטארט־אפ הישראלי שרוצה לתפוס את אדוארד סנודן הבא – לפני ההדלפה

ממעילת המיליונים ב-yes, דרך אתי אלון בבנק למסחר ועד לענת קם והמסמכים המסווגים בצה"ל – לאף אחד אין עדיין פתרון לאיום העובד הפנימי ● הסטארט־אפ אינסייבר מנסה לזהות את העובד הסורר עוד לפני ביצוע העבירה – ולהגן על ארגונים מפני תקיפות מבית

אמיתי זיו

אחד האתגרים הבלתי פתורים של ענף הסייבר, ושל ארגונים בכלל, הוא איום העובד הפנימי – מה שמכונה "insider threat". לא צריך ללכת רחוק כדי למצוא דוגמאות: לפני כמה חודשים עובד בחברת הסייבר ההתקפי NSO גנב את קוד המקור של נשק הסייבר המרכזי של החברה, וניסה למכור אותו ברשת האפלה; ב-2014 גנבו שני עובדי לאומי קארד מאגר מידע של 2 מיליון לקוחות החברה, וניסו לסחוט אותה תמורת אי־פרסום המידע; עוד באותה שנה נחשף כי עובדת yes בשם פזית ולד מעלה ב-31 מיליון שקל מכספי החברה; ב-2009 חיילת משוחררת זוטרה בשם ענת קם הדליפה לתקשורת אלפי מסמכים, וחשפה שאלוף פיקוד המרכז מורה על חיפולים בניגוד להוראות בג"ץ, בעוד שניתן היה לעצור את המבוקשים.

וכמובן שיש את אדוארד סנודן, המדליף המפורסם בהיסטוריה, שלקח מסוכנות הביון האמריקאית NSA כמיליון וחצי מסמכים, העביר אותם לעיתונות – ושינה לעד את השיח הציבורי על מעקב המוני בעידן המודרני.

"עם כל הרעש שהסייבר עושה, והדימוי של האקרים עם קפוצ'ון, 50% מהנזק הארגוני הוא מבפנים ולא מבחוץ. אם בתכלס סופרים נזק בכסף, האיום הפנימי לא פתור, הוא פרוץ", מסביר אבישי רוטמן, מייסד שותף בחברת אינסייבר (InCyber), שהוקמה כדי להתמודד עם איום התוקף הפנימי. "המעילה יכולה להיות בכסף, במידע או בקניין רוחני של החברה, אבל הנקודה החשובה היא שבן אדם לא נכנס יום אחד לעבודה ומחליט לגנוב מיליון דולר.

"העובד הזה קודם כל בודק את הרדאר של הארגון – איזו פעולה מקפיצה דגל אדום במערכות, איזו פעולה מצריכה אישור מנהל וכדומה; כך, אם למשל משיכה של 20 אלף שקל מצריכה אישור מנהל, הוא יעשה הרבה טרנזקציות של 19 אלף שקל. הבדיקות האלה של העובד הן אנומליות בהגדרה".

לזהות את התוקפים על פי ההתנהגות בשגרה

אינסייבר מנסה לזהות את התוקף מבפנים על בסיס מערכת הלוגים (log) של הארגון, שמתעדת כל פעולה בו – כל כניסה לחשבון, בירור יתרה או הדפסת מסמך. "הטכנולוגיה של אינסייבר אינה מבוססת על כללים המוגדרים מראש", אומר רוטמן. האלגוריתם מסתכל חצי שנה אחורה על שני דברים – הוא משווה את הפעילות של העובד לעצמו, ומשווה את הפעילות של העובד לעובדים המקבילים אליו בארגון.

"קח לדוגמה את אתי אלון, שהיתה האחראית למעילת ענק בבנק למסחר, שהובילה לקריסתו. מה היתה השיטה שלה? היא פתחה קובץ וורד והקלידה לתוכו את היתרה של הלקוחות, שלא היתה שם באמת. מספר הפעמים שהיא פתחה קובץ וורד ביום, פעולה שנרשמת בלוגים, היתה חריגה לעומת עובדים אחרים. אלירן רוזנס מלאומי קארד הוריד בהדרגה עוד ועוד רשומות של לקוחות לכונן C, המקומי, ובסוף פירק את הכונן עם מברג וטס לתאילנד – גם זו פעילות חריגה. אם יום העבודה הוא בין 8:00 ל-17:00, ועובד מסוים מבצע הרבה פעולות בין 16:45 ל-17:15, או בזמן ארוחת הצהריים, זה משהו חריג".

המערכת של אינסייבר בנויה, כאמור, על לוגים שהחברה מקבלת. ואולם לרוטמן חשוב להדגיש כי זו מערכת שמתחשבת בפרטיות העובד. "מבחינתנו, אפשר לקבל את המידע מותמם (אחרי שהוא עבר אנונימיזציה) בלי אף נתון מזהה של העובד. בגלל זה אנחנו גם לא סורקים רשתות חברתיות וכדומה. אנחנו מקבלים לוגים ומוצאים רשימה של עובדים שהם High Risk. בארגון של 5,000 עובדים, זה יהיה 15 עובדים בסך הכל".

בפתרון של אינסייבר יש 15 פרמטרים שונים, שאותם ניתן להצליב עם דירוג האשראי של העובד – ולזהות כך, למשל, עובד במצוקה כלכלית – וכן עם הציון שהעובד קיבל במבחני האישיות שערך הארגון, נתוני מיקום ושעות ופרמטרים נוספים. "עשינו בדיקה על מידע של בנק ישראל מ-2015", מספר רוטמן. "מתוך 5,000 עובדים, הצבענו על עשרה מסוכנים. מסתבר שאחת מהעובדות שהופיעה ברשימה אכן מעלה".

הפתרון של אינסייבר זמין גם כשירות בענן, אבל מרבית הלקוחות יעדיפו ככל הנראה פתרון מבוסס שרת, שמותקן בארגון. "המערכת לא עובדת בזמן אמת, ואנחנו ממליצים ללקוח – מנהל הסיכונים בחברה, סמנכ"ל הכספים או חברת הביקורת – להריץ בדיקה פעם בשבועיים על המידע שנוסף לאורך אותה התקופה".

החברה תציג את המוצר שלה לראשונה בתערוכת HLS, שצפויה להיפתח היום בתל אביב.

אדוארד סנודן. המדליף המפורסם בהיסטוריה צילום: אורנשטיין חושן תק

צילום: נופר חן

הגורמים לעליית האיום הפנימי בארגונים

- מספר גדול של עובדים עם הרשאות גבוהות
- ריבוי מכשירים עם גישה לרשת
- מורכבות טכנולוגית
- גידול בכמות המידע האישי
- הכשרת עובדים לקויה

מקור: CA

אבישי רוטמן: "עם כל הרעש שהסייבר עושה והדימוי של האקרים עם קפוצ'ון, 50% מהנזק הארגוני הוא מבפנים. אם סופרים נזק בכסף, האיום הפנימי פרוץ"

האיום הפנימי יכול להיות עובד שנפל בפח

במחקר של מקינזי מספטמבר, שעסק באיומים פנימיים, נבחן מאגר מידע של 7,800 אירועי סייבר מהשנים 2012-2017. במחקר נמצא כי "50% מהאירועים שנסקרו הכילו מרכיב משמעותי של תוקף פנימי". במקינזי מכירים בכך שהאיום הפנימי יכול להיות עובד שנפל בפח של רמאים מבחוץ או נזק מתוך חוסר זהירות, אבל יכול להיות גם גורם עוין בתוך החברה.

"תוקף פנימי לא תמיד רוצה בהכרח לפגוע בארגון. הוא יכול למשל להשתמש במידע על לקוחות לצורכי הונאה כדי להעשיר את עצמו, אך לא כדי לפגוע בארגון. במקרים אחרים, העובד יכול לחפש תשומת לב (זו אגב התזה שהציג רם בן ברק, לשעבר המשנה לראש המוסד, לגבי סנודן; א"ז) או שיהיה לו 'תסביך גיבור' והוא עשוי לחשוב שהוא פועל לטובת הציבור", נכתב במחקר של מקינזי. "התוקף הפנימי לא מתעורר כך בוקר אחד. ברוב המקרים מדובר בעובד נורמטיבי, שהופך בהדרגה לכזה, לאורך חודשים או שנים, ועם נורות אזהרה על אירוע פנימי מתפתח".

אינסייבר לא פועלת לבד בתחום. יש לא מעט פתרונות סייבר מבוססי לוגים וגם לא מעט פתרונות מבוססי התנהגות עובד (UBA). הבעיה היא שהרבה מהמוצרים האלה, לפי מקינזי, סובלים מהתראות כוזבות, מה שגורם באיזשהו שלב לאובדן אמון במערכת. רוטמן מצביע על הבדל נוסף בין הטכנולוגיה שלו לאחרות. לדבריו, "רוב הפתרונות מסתכלים החוצה, ומנסים לעשות גם וגם (לזהות מתקפות מבפנים ומבחוץ; א"ז), אנחנו מסתכלים רק פנימה".

חברת הסייבר הבינלאומית Trustwave חשפה לאחרונה ברשת האפלה כמה מודעות גיוס של עובדים בחברות ספציפיות, כמו "דרוש עובד ותיק מחברת טלקום", או הבטחה לתשלום של "2,000 דולר לחודש עבור עובד בנק לשעה עבודה בשבוע". זיו מדור, סמנכ"ל המחקר ב-Trustwave אמר ל-CNBC כי "מגייסים כאלה ברשת האפלה מחפשים גישה למשימות שונות, כמו הגדלת מסגרת המשיכה בבנק או עוד מידע פנימי על מטרה. הם מחפשים גם אנשים שיוכלו להסביר על איך להתחבר לחשבונות מסוימים".

אמזון פתחה בספטמבר בחקירה נגד עובדים ששחרו בסודות על מערכת המסחר של החברה תמורת כסף. עוד באותו חודש, עובד ממוצא סיני באפל גנב וניסה להבריח לסין מסמך בן 25 עמודים שבו תוכנית של לוח אלקטרוני לרכב האוטונומי של החברה.

"הרעיון לעסק התחיל בפרשת ענת קם"

את אינסייבר הקימו יזמים ותיקים. בראש החברה עומד ד"ר אברהם (איב) גיל, 70, ממקימי מכון לב בירושלים, ששהה שנים ארוכות בחו"ל וכעת חזר לישראל. רוטמן היה חוקר משטרה, אחר כך יועץ בתום מניעת הונאות וניהול סיכונים, ובמשך כמה שנים עבד כאחראי תחום מניעת ההונאות בפלאפון. המייסד השלישי הוא גיא הולצמן, שמפעיל את הפעילות האמריקאית של החברה. מלבד היזמים, ועוד עובד אחד, שאר הפיתוח של החברה נעשה בהודו.

"החברה פותחה מהון עצמי ועל בסיס קניין רוחני אקדמי של גיל, ומאז גייסנו מיליון דולר מאנג'לים", מספר רוטמן. "הכל התחיל בפרשת ענת קם. ניסינו לחשוב איך אפשר למנוע מקרה כזה, ולהיפתח גם לעולמות העסקיים. המוצר פעיל מ-2017 ואנחנו מותקנים בשני בנקים, בפיילוט בחברת תקשורת, בחברת כרטיסי אשראי ובחברת ביטוח. יש עוד שני בנקים שאנחנו בתהליכי פיילוט מולם. אגב, הדגש על בנקים הוא בגלל שאלה ארגונים שהרגולציה מחייבת אותם להיות פרואקטיבים במניעת הונאה – אבל אנחנו מוכרים לכל ארגון שמעסיק יותר מ-500 עובדים".

על פי מחקר של מקינזי, "התוקף הפנימי לא מתעורר כך בוקר אחד. ברוב המקרים מדובר בעובד נורמטיבי, שהופך לכזה לאורך חודשים או שנים, עם נורות אזהרה