

היכולת ליישם מנועים אנליטיים שמאתרים אנומליות, תבניות מוכרות או פרופילים מזוהים, ויכולים להתריע על פעילות חשודה, לאמוד את הסיכון בזמן אמת ולמנוע אותו. המערכות הללו מבוססות על תפיסת מודיעין, ולא על תפיסת הגבלת גישה - ומכאן ההבדל המהותי ביניהן ובין מערכות אבטחת המידע המסורתיות."

בהתאם לכך, אמר ד"ר קוזלובסקי, כי ניתן לזהות שתי מגמות הפוכות בקרב חברות האבטחה היום: "המגמה הראשונה כוללת חברות סטארט-אפ שבוחנות מערכות לגאסי, מזהות את החורים והחולשות שמצויות בהן, ומייצרות פתרון בהתאם. המדובר בפתרונות שנועדו להקשיח ולהגביר את רמת האבטחה במערכות שנבנו, כנראה, בצורה לא מספיק



ד"ר נמרוד קוזלובסקי

מאובטחת. במילים אחרות: מדובר על פתרונות שמסתכלים על אחורה." המגמה השנייה דווקא מסתכלת קדימה. מדובר בגל של חברות שמנסות לחזות לאן השוק הולך, ולפתח בהתאם פתרונות אבטחת מידע שיוטמעו מראש בתוך מערכות העתיד. הרבה מאוד מהדיון בחברות הללו עוסק באופן שבו הולך להיראות ה-'אינטרנט של הדברים' (The Internet of Things), כיצד יראה המעבר שלנו לענן בצורה מלאה ואיך תיראנה מערכות משובצות מחשב בעתיד, כולל מערכות תשתיות קריטיות. הרעיון, כאמור, הוא לשלב מלכתחילה את היבטי אבטחת המידע בתוך המערכות הללו."

ד"ר קוזלובסקי ושותפו בחממת הסייבר של JVP, יואב צרויה, הגיעו השנה ל-RSA Conference לא רק כדי להתעדכן בחידושים ולהשתתף בפגישות, אלא גם כדי להכריז על הסטארט-אפ הזוכה בתחרות ה-CyberTition שערכו בחודש האחרון. המנצחת בתחרות, חברת טיטניום מבאר שבע, זכתה בהשקעה של מיליון דולר ובהצטרפות לחממה. קוזלובסקי ציין, כי כ-50 הצעות הוגשו לתחרות ומתוכן נבחנו כ-35 הצעות שעמדו בקריטריונים.

לדבריו, "סטארט-אפ חייב להיות קשוב לשוק כבר מהרגע הראשון. במקרים רבים יש צרכים שהיזמים מדמיינים שהשוק צריך או מזהים נקודה שהם חושבים שהיא בעייתית, אבל עד שלא מקשיבים ללקוח באמת, מבינים מה מטריד אותו, איך הוא רואה את האינטגרציה של המוצר והאם יש או אין לו תמריץ להטמיע אותו - הם לא באמת יודעים איך המוצר שלהם ייתפס. לכן, ההמלצה החדה ביותר שלנו לסטארט-אפים, היא לדבר עם הלקוח מתחילת הדרך ולקבל פידבק. ההקשבה הזו היא חיונית בשלב הראשון. היזמים חייבים להיות נכונים לשנות את המוצר, לשנות את הצורה שבה הם מציעים אותו ולשנות את צורת האינטגרציה שלו. הגמישות הזו שקיימת אצל סטארט-אפ בראשית הדרך, תעלם בשלב מאוחר יותר בחייו - ולכן חייבים לנצל אותה כמה שיותר מוקדם."

\* הכותב הוא שליח אנשים ומחשבים לארצות הברית

"עד שיהיו נורמות, התעשייה תמשיך להימצא בין הפטיש לסדן", אמר צ'רני. "היא יכולה להצפין מידע, לדוגמה, ובכך להקשות על הממשלה לגשת לנתונים שעלולים להיות קריטיים, או לא להצפין את המידע - ולסכן במידה רבה את הפרטיות של הלקוחות שלה. ברור שחייבים לנהל דיון ציבורי בהשתתפות כל הצדדים, וברור שזה חייב לקרות מיד. עלינו לקבל החלטות ולקבל אותן עכשיו, כי המצב הנוכחי לא יכול להמשך לאורך זמן."

## "השוק עובר מאבטחת מידע לאבטחת סייבר"

"שוק האבטחה העולמי עובר בהדרגה מתפיסה של אבטחת מידע, לתפיסה של אבטחת הסייבר.

ד"ר נמרוד קוזלובסקי:

"חלק גדול מהתוכנות,

כוח המיחשוב והאחסון,

נמצאים בענן. הרבה

מאוד מכשירים הם

מכשירים שהמשתמש

מביא אל תוך הרשת

הארגונית והם לא

מנוהלים על ידי הארגון.

בנוסף, אנחנו צריכים

להשתמש במשאבים

משותפים, שהם לא

בטוחים בהגדרתם"

במקום גישה של בניית גדר, עוברים לגישה של הצבת מצלמת ניטור חכמה, כך אמר ד"ר נמרוד קוזלובסקי, שותף בחממת הסייבר של קרן JVP בבאר שבע. לדבריו, "הגישה החדשה הזו מציבה את מדינת ישראל במצב מצוין, כי חלק גדול מקהילת הסייבר שלנו מגיע מיחידות מודיעין שזו התפיסה שלהן. זה הוליד גל חדש של יזמות בתחום האבטחה הפרואקטיבית - וחלק לא מבוטל ממנו מקורו בארץ."

ד"ר קוזלובסקי אמר את הדברים בראיון לאנשים ומחשבים, שנערך במסגרת הכנס "אבטחת המידע המסורתית עסקה בעיקר בהגנת הגישה", פירט קוזלובסקי: "איך אני מגדיר גישה למערכת הארגונית ומתחם את הארגון? איך אני מגדיר מי מותר גישה

ומי אסור גישה? איך אני מגדיר את האופן שבו ניתן לגשת לנכסי המידע שלי ובאילו תנאים? בפועל, מדובר במוצרים שמתמקדים בעיקר בשליטה, ניהול והגנה על הגישה. נראה שהדור הזה של המוצרים עובר מהעולם, ויש לכך שתי סיבות עיקריות: הסיבה הראשונה היא, שקשה לתחזק ולנהל את המוצרים הללו. הסיבה השנייה היא, שעולם ה-ID השתנה."

הוא הסביר, כי "לפני 15 שנים, רוב המחשבים שהיינו משתמשים בהם היו מנוהלים על ידי הארגון - הוא היה שולט בתוכנה ובהגדרות האבטחה. היום אנחנו עדים לסביבת ID שונה לחלוטין. זו סביבה שבה הארגון כל הזמן מתחבר החוצה. חלק גדול מהתוכנות, כוח המיחשוב והאחסון, נמצאים בענן. הרבה מאוד מכשירים הם מכשירים שהמשתמש מביא אל תוך הרשת הארגונית והם לא מנוהלים על ידי הארגון. בנוסף, אנחנו צריכים להשתמש במשאבים משותפים, שהם לא בטוחים בהגדרתם."

## תפיסה אחרת של אבטחה

כתוצאה מכך, הוסיף ד"ר קוזלובסקי, "נדרשת תפיסה אחרת של אבטחה, שלא עוסקת רק בניהול הגישה. הנחת היסוד של הגישה הזו היא, שהגורם התוקף יצליח להיכנס אל המערכת, אם הוא לא כבר שם. זה מצריך פרדיגמה חדשה, פרואקטיבית, שמניחה שצריך לא רק לדעת לנטר ולזהות בזמן אמת אירוע אבטחת מידע, אלא גם למנוע אותו בזמן אמת. זה מצריך תפיסה הרבה יותר מודיעינית, של איסוף נתונים בזמן אמת מנקודות מידע ושיתוף המידע הזה. כך, נדרש לפתח את