

פיננסיות גדולות. המודל שלה מבוסס על אלגוריתם מתמטי שפותח במטרה לאתר אנומליות ברשת והתנהגות חריגה בסביבת Big Data. הפתרון מזהה מתקפות מחד לצד הפחתת שיעור התראות שווא מאידך. לדברי גזית, "מערכות של תשתיות חיוניות, שנשלטות באמצעות מערכות בקרה תעשייתיות, בהן פרוטוקול ה-SCADA שולט, חשופות לפגיעה שעלולה להשבית את השירות החיוני ואף לגרום לנזק פיזי. בנוסף, נדרש להגן מפני תקיפות על מערכות אלחוטיות ותחנות שידור ניידות, שימוש ברשתות חברתיות לצרכי הפצת רוגלות, נזקקות ותקיפות של שירותי אחסון ומיחשוב ענן".

"תקיפות מצליחות לחדור לרשתות הארגוניות ולמחשבי הקצה למרות מערכות ההגנה כי ההופעה הראשונית של הנוזקות נראית חוקית ותקינה", הוסיף. "כמו כן, רוב המערכות המבצעיות בנויות לטיפול בסוג מסוים של מתקפה ואין להן יכולת לטפל במגוון של מתקפות שונות שיש להן מוטציות רק התנהגות א-נורמלית שלהן בהמשך שהותן בארגון היא שתסגיר אותן. מכאן, אם תהיה אפשרות לאבחן את ההתנהגות השונה באוקיינוס של נתונים, ניתן יהיה להתגונן מפניהם". הוא סיכם באמרו כי "המתקפות הן חד פעמיות ולכן, יש להיזהר מהדברים שאין ידיעה שלא יודעים אותם".

## איומי הסייבר בכלים בלתי מאוישים

**שי בליצבלא, מנכ"ל מגלן טכנולוגיות מידע, תיאר בפני המשתתפים את איומי הסייבר הטמונים בכלים הבלתי מאוישים. "המערכות בכיפת ברזל סגורות, אבל יש מערכות צבאיות פתוחות, כי נדרש להעביר מידע ונתונים בזמן אמת. ככלל, המצב כיום הוא שהתעשייה הביטחונית המסורתית מתחילה להיפרד מהסגירות הצבאית", אמר.**

לדבריו, "המצב בכלים הבלתי מאוישים הוא שרמת היישומים בדרך כלל מאוד נמוכה ובשל כך, רמת ההיפגעות הפוטנציאלית בהם מאוד גבוהה". בנוסף, ציין בליצבלא, "גם מערכות ההפעלה משובצות המחשב ושכבת החומרה פריצות".

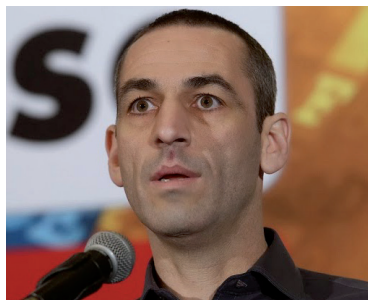


שי בליצבלא

"אין מזל"ט בלי תוכנה", סיים. "עשינו כמה בדיקות עם כלים בלתי מאוישים. איתרנו את אזור מפתח ההצפנה. אמנם לא הצלחנו לשבור את ההצפנה, אבל הצלחנו להזריק לתוך מערכות המיחשוב של הכלים נזקות. כשמטפלים בכלים בלתי מאוישים, נדרש לטפל גם בהיבט האבטחה הפיזית וגם בהיבט אבטחת ה-IT שלהם".

## "אין אבטחת מידע במערכות התפעוליות והלוגיסטיות"

"הארגונים נפתחים למערכות התפעוליות שלהם, דוגמת ספר טלפונים ארגוני, או מערכות לוגיסטיות. בכל אלה - אין מערכות אבטחת מידע", כך אמר יוסי שנהב,



יוסי שנהב

מנהל ייעוץ בקומודו. "לדברי שנהב, "איומי אבטחת המידע והסייבר הולכים ונהיים מתוחכמים יותר ויותר. הדבר דורש היערכות מעמיקה ונרחבת יותר מצדם של ארגונים ומנהלי אבטחת המידע שלהם". דוגמה לכך שעולם

הוא אמר, כי "הסטארט-אפ המתמודד עם המתקפות נדרש לעמוד בתנאים הבאים: טכנולוגיה חדשנית וייחודית בתחום הסייבר או אבטחת המידע; צורך שוק שמצדיק את פיתוחה של הטכנולוגיה הזו; יתרון תחרותי צפוי בתחום הפעילות של המיזם; צוות מקצועי בעל ניסיון בתחום הפעילות המוצע; יכולת לפתח אבטיפוס של המוצר בתוך שנה; והמיזם טרם קיבל השקעה מגוף מוסדי וסך ההשקעה המצטברת במיזם מגוף שאינו מוסדי, אם הייתה, לא עולה על חצי מיליון דולר. אנחנו מחפשים נמרים קטנים", סיכם.

## "הביטקוין ישנה את כללי המסחר בעולם"

"זה רק עניין של זמן עד שהביטקוין ישנה את כללי המסחר בעולם. Cryptocurrency, מסחר במדיום דיגיטלי, נמצא כאן כדי להישאר", כך אמר **יורם גולנדסקי**, מנכ"ל Security Art, שנוסדה לפני ארבע שנים ולפני חצי שנה נכרשה על ידי



יורם גולנדסקי

קבוצת HMS. בדבריו תיאר גולנדסקי את דרך המסחר עם ביטקוין: "תהליך הכרייה שלו נעשה על ידי כוח מיחשוב. מי שכורה את המטבע - הוא בעליו. מדובר במטבע סחיר בין ארנקים דיגיטליים, כאשר לכל ארנק יש מפתח ציבורי ומפתח פרטי. אם

מישהו רוצה להעביר למישהו כסף, הטרנזקציה תהיה במפתח ציבורי ואילו החתימה תהיה במפתח הפרטי. בסוף, הכסף יהיה שייך לאותו מישהו".

לכל מטבע, אמר, יש היסטוריה של מסחר עמו, "וההיסטוריה הזו היא היוצרת את האמון בין הסוחרים בו". הוא הוסיף כי "אם אני רוצה להעביר לאדם ביטקוין בשווי סכום כסף מסוים, תבוצע בקרה שיש לי בארנק את הכסף. אין אוברדראפט. ככל שיהיו לי יותר אישורים, כך אצבור יותר אמון והעסקה לא תיפול".

לדברי גולנדסקי, "הביטקוין הוא כמו כסף אמיתי, יש לו ערך שנקבע כמה פעמים ביום, על פי דרישה. הכסף לא יכול להיות ליותר מאדם אחד בו זמנית והוא ניתן להעברה. מצד שני, המטבע הזה לא דומה לשום מטבע אחר. אין בנק מרכזי, אין רגולציה, אין מי שמאשר או לא מאשר, אין יכולת להחליף שטר קרוע ואובדן המפתח הפרטי משמעו אובדן הכסף".

גולנדסקי סיים באמרו, כי "בעולם הפיזי אנחנו משלמים עמלות על הכסף, אבל בעולם הווירטואלי, מושג העמלות לא קיים. תידרש רגולציה לניהול התחום, כי אנחנו רוצים לשמור על כספנו. עולם ה-Cryptocurrency הוא הבינוס הנכון, זהו עולם הזז במהירות, עם התפתחויות מדהימות".

## "יש בעולם אין סוף איומים"

**מארק גזית, מנכ"ל ThetaRay, התייחס לאבטחת מידע ולמתקפות קיברנטיות.** הוא אמר כי "העולם מתמלא כל הזמן בדברים חדשים, כולל



מארק גזית

אין סוף איומים. כתוצאה מהם נוצרה כמות גדולה של וקטורי תקיפה".

הוא ציין כי ThetaRay "פועלת למניעת מתקפות יום אפס ומתקפות APT (Advanced Persistent Threat) על מערכות תשתית קריטיות, מתקנים אסטרטגיים, מערכות תקשורת ומערכות