

אבל עדיין זה העלה את המודעות ואי אפשר להתעלם מכך שזה שיפר את המצב תקציבית, אבל הווירוס של היום הוא לא הווירוס שרלוונטי מחר."

## אבל, זה יכול לקרות

למרות שה-7 באפריל עבר וכבר חלף מזמן, עם תוצאות בהחלט שוליות, בליצבלאו לא רואה את התמונה מבעד למשקפיים ורודים. הוא בהחלט חושש שבסופו של דבר התקפת האקרים מרוכזת על תשתיות האינטרנט והתקשורת של ישראל יכולה לבוא ולפגוע באמת. "אני אגיד לך דבר שאני חוזר עליו בכל מקום: רמת אבטחת המידע ואיכות אבטחת המידע ב-100 או ב-500 הארגונים הגדולים בישראל היא לא יותר מאשר בינונית", הוא טוען.

### ממה זה נובע?

"מדבר אחד יסודי ומושרש, שהוא אפילו לא משתנה במשך השנים: רמת יישום נמוכה".

### מתוך מודעות?

"לא, מתוך אי הבנה. אתה יודע, גם לא מחוסר הבנה, אלא מגישה שנוקטת שעדיף לבצע התקנה בסגנון ישר מהקופסה, בלי להגדיר תצורה ולהתעמק בהגדרות חד ערכיות ולבצע התאמות שבאמת דרושות לארגון המסוים. קח את צ'ק פוינט, זה מוצר פיירוול מהטובים בעולם, ואין כל ויכוח. עם זאת, קביעת התצורה לבנק א' לא מתאימה לבנק ב', אבל מבחינת האינטגרטור זה אותו פרויקט - שני בנקים שצריך להתקין בהם את התוכנה".

### זו בעיה של חינוך?

"זה חינוך. זו מילה טובה. זה יותר מהכל עולם אבטחת מידע שמושפע מהחלטות עסקיות. קשה מאוד לאנשי אבטחת מידע להתמודד עם זה. בא המנכ"ל ואומר לאיש אבטחת המידע שלו, 'אני צריך את השירות מחר', וזה מה שהכי מעניין אותו. אני יכול להבין את הגישה הזאת, אבל הדבר גורם לקיצורי דרך בעניין האבטחה. יומיים אחר כך הם נפרצים, וזה חוזר כמו בומרנג".

### אפשר לשבור את המעגל הזה?

"זה לא מסובך כל כך. פעם, בעולם התוכנה היה נהוג להשתמש בנהל בדיקות קבלת מערכת. צריך לחזור לביצוע של בדיקות קבלה פרטניות. צריך להחזיר את האינטגרטור לתקן אם מתגלות בעיות, ואם צריך אפילו לקנוס אותו, או לקבוע איתו מראש שהוא מקבל את התשלום רק לאחר השלמת הביצוע במלואה לפי הצרכים האמיתיים. צריך להפסיק ליישר פינות בגלל צורך עסקי, כי כשהרשת נפרצת כל העולם העסקי בטל בשישים".

## להשתמש במומחים מנוסים

42 עובדים יש כיום במגלן, שכבר קיימת 14 שנים. שליש מהפעילות של החברה מתרכז במחקר. בחברה נמצא מרכז בדיקות אבטחת המידע הגדול בארץ, "ולפי SC Magazine, זה לפחות לפי מה שאני יודע, אנחנו מחמש החברות הגדולות בתחום באירופה", מספר בליצבלאו. "הם מודדים אותך מקצועית ולא כלכלית, כמה תרגילי תקיפה מבוקרים עשית השבוע ללקוחות שהם ברשימת החברות הגדולות. יש כללים מאוד נוקשים, ומצד שני זה נותן אינדיקציה ברורה מאוד. יש כאן בארץ לקוחות רבים, וזה לא יאומן לרעתי, שבהם נמנעים מלקחת את מגלן לבדיקת המערכות בטענה שהם מפחדים מהתוצאה, מהאמת הערומה. אני לא מלין שלא לוקחים אותי, כי תודה לאל יש לי מספיק עבודה, אלא על התופעה: שמפחדים לחשוף את האמת. ממש ככה".

## זה לא ממש מקצועי, אם זה נכון מה שאתה מספר.

"נכון. וזה מעבר לכך, לצערי לא תמיד מי שמטפל בנושא באמת מקצועי. צריך להביא מומחי אבטחת מידע מנוסים ועתידי ניסיון להתקנה וגם לבדיקת המערכת, ויש כאלה. קח דוגמה: כל עובד שמגיע למגלן מקבל 100 אלף שקל בחצי השנה הראשונה לצורך לימודים והכשרה. זה החוסן שלנו. בלי זה אי אפשר למכור שירות גבוהה, כי בסוף, כשאני בא ללקוח ואומר לו שמצבו גרוע, אני רוצה להביא לו מישהו שיידע להרים אותו, להגדיר עבורו גם את הפרט הכי קטן במוצרי האבטחה שלו".

### ומה קורה בתחום הממשלתי?

"אתה מתכוון לתהילה? תהילה עשתה לראייתנו בשנתיים האחרונות שינוי מקצועי איכותי ומדהים. היא עשתה סדר בבלגאן. עשו שינוי ארגוני מקצועי מקצה לקצה, שינו את הפרסונה, שזה הדבר הכי מהותי במשרדי ממשלה ומסובך מאוד. הביאו כוח אדם ממש איכותי. לאנשים החדשים הללו אכפת מהמערכות ולא מעצמם. הם יושבים בדיונים והם מתעקשים על איכות. זה הגוף הכי חשוב, זה הפנים שלנו, וטוב שזה כך. והדבר הכי חשוב, שזה יימשיך ויחזיק מעמד. בגופים כאלה יש לפעמים צניחה, ושם צריך שהם ישמרו על המתח הגבוה".

### אז הם מוכנים לאירוע הסייבר הבא?

"התכוונת לאירוע אבטחת המידע הבא".

### למה לא סייבר?

"הרוב המכריע של מה שאנחנו מכנים אירועי סייבר, התקפות סייבר וריצות סייבר, הם אירועי אבטחת מידע. נקודה. בסביבות 5% מהאירועים לכל היותר הן התקפות סייבר. אנחנו מתייחסים לסייבר כשיש לנו או תווך לוגי שמחובר לתווך פיזי, או תווך לוגי עם דילוג על תווכים. סייבר זה בעצם תקיפה שמצליחה לפרוץ את גבולות המערכת שאליה מתחברים, או אפילו את גבולות המרחב של המערכת, ולהשפיע על מערכות שלא מקושרות ישירות אליה או במרחבים אחרים, כלומר לפגוע בשטחים נוספים. בעולם הפיזי/לוגי זה די מוגבל, זה להשתלט על המחשב ששולט על המחשב ששולט במערכות, ואז להפסיק את המערכות עצמן, הפיזיות. בעולם הווירטואלי זה להשיג מידע, כשמידע כיום זה כסף עובר לסוחר".

### אז זה רק שם יפה?

"מאוד".

### ובכל זאת, קנה מידה גדול יותר?

"אולי, וגם השפעות יותר גדולות על הסביבה. תראה. בשנת 2000 התרחשה התקיפה המכוננת שגרמה הכי הרבה נזק, כשהאקר בשם מיקסטר שיתק בעזרת התקפת מניעת שירות את יאהו, את אמזון, את אי-ביי ואת CNN וגרם נזק של מיליארד דולרים, שזה היה סכום מטורף לאותה תקופה. הטכניקה נותרה אותה טכניקה, ואיך קראו לאירוע? אבטחת מידע".

### אומרים שהתקיפות הגדולות מתבצעות בעזרת מיליוני מחשב זומבי, של צרכנים. מה הצרכן צריך לעשות?

"צריך לזכור משהו יסודי. כל מערכות ההפעלה, ובטח חלונות, עתידות רכיבי אבטחת מידע ויכולות הגנה בלי שום מוצר נוסף. צריך לזכור, צרכן, לעשות שני דברים: להפעיל את המנגנונים הללו ולדאוג שהם יתעדכנו אוטומטית. זהו. זה אמור להפסיק".