מעריב - סופהשבוע
עמוד 36 , 06/10/2017 , 23.36 x 32.91
כתבים: הדר חורש
60533252

הדר חורש
דירקטור חיצוני

הטעות של אבו

מה ניתן ללמוד מההשקעה הפרטית של מנכ"ל דלק אנרגיה בניירות הערך של שותפות הגז "דלק קידוחים" ■ וההאקר המקצועי שרון נמירובסקי מסביר מדוע בלתי אפשרי להתחבר לאינטרנט ולהיות מוגן בו־זמנית

לא קשה להבין מדוע בחר הטייקון יצחק תשובה לקדם את המנהל הצעיר יוסי אבו לתפקיד מנכ"ל דלק אנרגיה. הוא איש נמרץ ובעל קסם אישי רב. תפקידו העיקרי הוא לשווק את הגז מהמאגר שבו שותפה דלק אנרגיה, "תמר", ולסגור עסקאות עם הלקוחות. הרווחיות העצומה של דלק מוכיחה שאבו עושה עבודתו נאמנה. אבל לא בטוח שאתם רוצים לתת לו לנהל את תיק ההשקעות שלכם.

בשנת 2011 היה אבו בטוח שיש לו רעיון להשקעה מבטיחה. הוא לווה מהבנק סכום עתק - 12 מיליון שקל - והשקיע את כולו בניירות הערך ("תעודות השתתפות") של שותפות הגז "דלק קידוחים", שבשליטת דלק אנרגיה. השותפות מחזיקה ב־22% ב"תמר". היו אז לאבו כל הסיבות להניח שמחיר ניירות הערך שרכש יאמיר בקרוב והוא יגרוף הון: המדינה שיוועה לגז, וכל מחיר שתשלם חברת החשמל יהיה נמוך ממחיר המזוט והסולר שנאלצה לרכוש מאז חדלה אספקת הגז ממצרים. הוא גם ידע שמצרים עצמה ומדינות אחרות באזור זקוקות מאוד לגז הישראלי שהתגלה זה עתה, ולזה שאולי עוד יתגלה.

אלא שהתחזיות לא התגשמו: התנהלות בעייתית של חברת החשמל והמוסדות שהיו אמורים לפקח על משק האנרגיה הניבה לחברות הגז חוזה חלומי עם חברת החשמל. אבל המחלוקת על מתווה הגז, בצירוף תגליות גז חדשות במצרים וסכסוך מתמשך עם טורקיה פוגגו את החלומות על הכנסות של מיליארדי דולרים מיצוא. התוצאה: אומנם שערי התעודות שרכש אבו האמירו זמן קצר לאחר העסקה, אבל הם חזרו וצללו. כשהגיע מועד פירעון מחצית ההלוואה שנטל מהבנק, 6 מיליון שקל, הוא עדיין לא הרוויח על ההשקעה והחזיר את החוב מכיסו. בשבוע שעבר הגיע המועד לפירעון מחצית החוב השנייה. אבו נאלץ לממש ערבות שקיבל מהחברה, וכך נמנע לפי שעה מהפסד נוסף.

אומנם שערי התעודות שרכש אבו האמירו זמן קצר לאחר העסקה, אבל הם חזרו וצללו. כשהגיע מועד פירעון מחצית ההלוואה שנטל מהבנק, 6 מיליון שקל, הוא עדיין לא הרוויח על ההשקעה והחזיר את החוב מכיסו

אבו. גם מנהלי החברות אינם יכולים לחזות את מחירי המניות שלהן
צילום: פלאש 90

מסקנות:

1. גם מנהלי החברות אינם יכולים לחזות את מחירי המניות שלהן. ונטייתם של משקיעים לפעול בהתאם למה שבעלי השליטה או בכירי החברה עושים, אינה ערובה לרווח.
2. אפילו אם נדמה לכם שאתם יודעים כל מה שאפשר לדעת על הזדמנות השקעה, כדאי תמיד לפזר היטב את השקעותיכם, ובמיוחד כשמדובר בהשקעות לטווח של כמה שנים.
3. אם כבר לקחתם סיכון בהשקעה ארוכת טווח, מוטב שלא לממנה באשראי בנקאי. במקרה של הפסד בהשקעה, עלויות האשראי רק מגדילות את הצרה. במקרה של אבו הסתכמה עלות הריבית לבנק בכ־1.5 מיליון שקל, נוסף על ההפסד מההשקעה עצמה.
4. למרות הפיתוי הרב, לא כדאי להשקיע במניות של חברה המעסיקה אתכם. אם יצוצו צרות בעסקים, אתם עלולים להישאר גם בלי עבודה וגם בלי חסכונות. במקרה של אבו, זהו סיכון שלא התממש.

האקר טוב

ההתקפה הבאה תבוא אחרי החגים, ואין לך הגנה נגדה. כך הזהיר אותי שרון נמירובסקי, האקר מקצועי, במשרדו שבמרכז תל אביב. אמרתי לו שאני מוגן מאחורי תוכנת אנטי־וירוס משוכללת וידועה שאני משלם עליה כמה עשרות דולרים מדי שנה, שלא לדבר על הדיפנדר החינמית של מיקרוסופט. "אם יש לך את הדיפנדר שלנו, אתה מסודר", הרגיע אותי איש אבטחה מהסניף המקומי של מיקרוסופט.

כמה ימים לאחר מכן הגיעה אלי במייל תמונה. היא צולמה בוודאות ממצלמת הרשת המותקנת במחשב הנייד שלי, שאותה לא הפעלתי מעולם, על ידי ההאקרים של ווייט האט, החברה שבבעלות נמירובסקי, ללא ידיעתי, ונשלחה אלי כהוכחה לעובדה שהאנטי־וירוס המשוכלל לא הצליח למנוע את הפריצה למחשב.

נמירובסקי. הקורבן חייב לשלם את הכופר // צילום: נדב כהן

האמת היא שהפריצה בוצעה בהסכמתי. וייתכן שלא הייתה יוצאת לפועל ללא סיוע קל: במכוון לחצתי על לינק שנשלח אלי, ובאמצעותו בוצעה הפריצה. ברור שזהירות בסיסית של משתמש מחשב מחייבת היום להימנע מלפתוח מייל ממקור בלתי מוכר, אבל גם זה לא יעמוד בפני האקר מיומן המבקש לתקוף אותנו. רבים מהווירוסים ומתוכנות הכופר חדרו לאחר שמשתמשים פתחו מיילים שהגיעו לכאורה ממקורות מוכרים ובטוחים.

ווייט האט מעסיקה האקרים מקצועיים, חלקם מגויסים מארגונים ממלכתיים העוסקים בהגנה או בתקיפות מחשבים. אנשי החברה עוסקים בתקיפת מערכות המחשב של הלקוח כדי לגלות פרצות אפשריות ולהתריע עליהן. תחום אחר הוא איסוף מודיעיני על מתקפות מתוכננות, אמצעי פריצה ופרצות חדשות המתגלות במערכות ההפעלה.

"אתה לא יכול להיות מחובר לאינטרנט ולהיות מוגן בו־זמנית", מסביר נמירובסקי, "ולא חשוב איזו תוכנת הגנה תחזיק. כל הארגונים האסטרטגיים והחברות הגדולות בישראל כבר ניתקו את המערכות המרכזיות שלהם מהאינטרנט, וגם זה לא בטוח לגמרי. אם אין מערכת הגנה היקפית, מישהו יכול להתגנב במסווה כלשהו לאחד המחשבים במערכת, להתחבר אליו ולהשתיל בו את התוכנה הפוגענית. אז הארגון חוסם את האפשרות להכניס דיסק־און־קי לשקע ה־USB, אבל התוכנה יכולה להתחזות למקלדת: המחשב מקבל את ההתחברות, כי הוא חושב שחיברו לו מקלדת תמימה".

יש הרבה דיבורים על מתקפות סייבר, אבל שומעים מעט מאוד על פריצות ותשלומי כופר להאקרים.

"בכל חודש משלמות חברות ישראליות הרבה מיליונים להאקרים שפרצו למערכות שלהן, הצפינו את התכנים באופן שאינו מאפשר לגשת אליהם, ודרשו כופר תמורת הפתיחה. אין דרך להתמודד עם תקיפה כזו לאחר שהיא מתרחשת. תוכנת ההצפנה היא צופן סימטרי, שחציו נמצא במחשב שנתקף וחציו האחר אצל התוקפים. אין דרך לדעת מהו הצופן מהצד השני, והקורבן חייב לשלם את הכופר או לוותר על המידע".

אבל היום יש לחברות וגם לאנשים פרטיים אפשרות לגבות את כל התכנים ולאחסנם בענן, שאינו נגיש לתוקפים.

"זה יכול לעזור, אבל לא תמיד. כאשר הקורבן מחובר באופן רציף או תכוף לגיבוי בענן, תוכנת ההצפנה יכולה להתחבר איתו לגיבוי ולהצפין גם את החומרים בענן. קשה יותר לעשות את זה אם ההתחברות היא קצרה וחד־פעמית: לשם כך יש להתנתק מהענן ולהתחבר אליו רק באופן יזום לצורך פעולת הגיבוי. מעטים מסוגלים לעשות זאת". ❖

hadarh002@gmail.com