איגוד האינטרנט הישראלי
ISOC-IL

האם לאזרחי ישראל יש כלים להתמודד עם איומי סייבר?

25/10/2020

בועז דולב, מנכ"ל ClearSky Cyber Security

יובל: ברוכים הבאים לנקודה IL, הפודקאסט של איגוד האינטרנט הישראלי שעוזר לנו להבין מה הן ההשפעות של האינטרנט על החברה, הכלכלה, הפוליטיקה והתרבות. אני דוקטור יובל דרור. היום אנחנו עוסקים באיומי סייבר. ואין אדם מתאים יותר לדבר איתו על הנושא הזה מהאורח שלי היום, בועז דולב, שהוא אחד מאנשי הסייבר הבכירים והמנוסים בישראל. הוא הקים את מערך ממשל זמין. קהילה שהיא תשתית האינטרנט של כלל משרדי הממשלה. במשך 15 שנה הוא טיפל בהגנה מפני תקיפות על אתרי הממשלה והקים את המערך המקוון שבו משרדי הממשלה נותנים שירותים באמצעות המערך הזה. כולנו משתמשים בו. ב-2011 הוא הקים את clear sky cyber security זו חברה שמספקת ללקוחות שלה מידע וכלים שמסייעים להם להתמודד עם ניסיונות תקיפה. בועז ברוך הבא לנקודה IL.

בועז: היי יובל, מה שלומך? אם אתה יכול, תחזור בבקשה עוד פעם על הפתיח, פשוט אהבתי אותו מדי.

יובל: אתה מוכן להיות לרגע רציני?

בועז: אני תמיד רציני.

יובל: כאשר אנחנו חושבים על תקיפות שהמטרה שלהן לחדור למידע שלנו, אנחנו בעצם חושבים על שלושה מעגלים. תקיפות שמנסות

לתקוף תשתיות של המדינה. תקיפות שמנסות לתקוף תשתיות של ארגונים ותקיפות שמנסות לתקוף אותנו באופן אישי. בוא נתחיל במעגל הראשון, מי תוקף את התשתיות של ישראל? ועד כמה ישראל מוגנת מהתקיפות האלה?

בועז: התקיפות על ישראל, נקרא לזה מדינת ישראל, מגיעות בעצם היום בעיקר משני גופים. גוף אחד זה בעצם מה שנקרא ארגוני הפשיעה, ארגוני הפשיעה הבינלאומיים, שהם מייצרים את תקיפות הכופרה הרציניות על חברות וארגונים בישראל. ממש עכשיו בשנייה הזאת שאנחנו מדברים אני מטפל בשני גופים שהותקפו בכופרה. וצריך לסייע להם בעצם גם בהתאוששות, גם ברכישת המפתח. ואני חושב שאם אנחנו מסתכלים כרגע על האיום הכי רציני, או הכי נפוץ שיש כרגע לישראל ועל חברות בישראל, אלה בעצם תקיפות הכופרה.

יובל: אנחנו מיד נגיע אליהם, אוקי, אז זה אחד, ארגוני פשיעה. מי הוא הגורם השני?

בועז: הגורם השני בעצם זה, מה שנקרא או מכונים, האויבים שלנו. לצורך העניין מדינות שרוצות לתקוף את ישראל, כשהמטרה בעצם שלהם היא כפולה. אחד זה לגנוב מידע. ריגול, מודיעין וכל מה שקשור אליו. והדבר השני זה הנושא של אולי גניבות כספיות. לצורך העניין, כשראינו השנה, או כשחשפנו את הפעילות של צפון קוריאה בישראל, לווה לזה בפירוש ניסיון גם לגניבה כספית.

יובל: את מה הם תוקפים?

בועז: הצפון קוריאנים מנסים קודם כל להגיע לחברות הביטחוניות בישראל, רוצים בעצם לגנוב את תכניות המקור של ה... לא יודע,

של כיפת ברזל. רוצים לגנוב את תכניות המקור של כל כלי נשק שהישראלים המציאו אי פעם. זה הדבר הראשון. והדבר השני זה באמת ניסיון לראות אם אפשר לגנוב קצת כסף גם מהחברות האלה.

יובל: חברת חשמל, מקורות? גם הם?

בועז: אז כן, חברות התשתיות הקריטיות נתקפות בדרך כלל על ידי מדינות או ארגונים שפועלים בשם מדינות. והמטרה בעצם זה לנסות להגיע למצב שבו אתה יכול לחבל בפעילות של מדינה, ברגע שאתה רוצה לעשות את זה.

יובל: עד כמה ישראל מוגנת מפני התקיפות האלו?

בועז: אני חושב שבשנים האחרונות... תראה, אני בדרך כלל לא אוהב את הממשלה, אבל אני מנסה כן לתת איזה שהיא מחמאה קטנה ברגע הזה. בשנים האחרונות מול מדינת ישראל... מדינת ישראל הקימה מערכי הגנה רב שכבתיים שמתחילים עם מערך הסייבר ואולי מגופי הביטחון שהיו קודם ולכל אחד מהם בעצם יש את הארגונים שלו. ובסך הכל אני חושב שהמערך ההגנה של ישראל הוא טוב היום. טוב זה ללא אומר שהוא טוב מאוד. יש עוד הרבה מאוד דברים שצריך לבצע, אבל יחסית למקומות אחרים אני חושב שאנחנו במצב טוב.

יובל: אז בוא נעבור לארגונים, המעגל השני. האם בעיניך ארגונים במדינת ישראל מוגנים מפני תוקפים?

בועז: ארגונים, בוא נגיד ככה, ארגונים שהוגדרו על ידי כל הגופים המדינתיים כגופים שצריך לשמור עליהם, לצורך העניין, חברת החשמל, דלק, אולי בתי חולים וזה, מקבלים בעצם מעטה, או

מטריה מדינתית שעוזרת להם לשרוד. החברות הפרטיות, כל ה... לצורך העניין המגזר העסקי, אני חושב שהוא במצב מאוד קשה. הוא לא ייצר עדיין את מעטה ההגנה המתאים. והתוצאה היא בעצם שהוא לא ממש מוגן. לעומת זאת המגזר הפיננסי, אם אנחנו מסתכלים עליו, כי הוא יודע שפשוט, אם הוא לא ידאג לעצמו פשוט יגנבו לו כסף, אז יש לו אינטרס מספר גבוה מאוד להגן על עצמו והם בשנים האחרונות ייצרו לעצמם מערכת הגנה מאוד טובה. אבל באמת המגזר התעשייתי בעיקר. החברות התעשייתיות, חלקן זה חברות של 30 שנה. נגיד אנשים מייצרים מקררים, לא יודעים לייצר הגנת סייבר ולכן המטרה... אני חושב שהם במצב מאוד קשה ואני חושב שהם מבינים את זה גם עכשיו. ועיקר התקיפות עכשיו, תקיפות הכופרה וזה, פוגעות בעצם בהם באופן מאוד קשה ומאלצות אותם ויאלצו אותם גם השנה וגם שנה הבאה להשקיע הרבה מאוד כסף בהגנת סייבר.

יובל: אז בוא באמת לרגע אחד נעשה זום אין על העניין הזה של הכופרה, האיום מספר אחד, כך אתה טוען, זה העניין הזה של ransomware בעצם מצפינים את כל המידע על המחשבים, על השרתים של הארגון, אומרים להם, אתם רוצים את המפתח? תשלמו. עד כמה האיום הזה באמת שכיח? ועד כמה הוא מסוכן?

בועז: הוא יותר מדי שכיח. זאת אומרת, באמת אני חושב שמדובר בעשרות חברות שמותקפות לדעתי בכל שבוע בישראל, במצב הנוכחי, כאילו כיום, עכשיו. זה היה פחות בעבר. עכשיו זה ממש הפך לסוג של מגיפה. אולי זה בהתאמה למגפת הקורונה. יש יותר לאנשים זמן לתקוף מרחוק. ויש הרבה... ואולי יותר אנשים בעצם

עובדים מרחוק ובעצם חושפים כך את הארגון לתקיפות סייבר. אז יש התאמה, אני לא צוחק הפעם. ואני חושב שזה בעצם מסביר לכל ארגון שלא דאג לזה שיהיה לו גיבוי כמו שצריך, אנחנו מטפלים היום בחברה שהיה לה גיבוי מצוין, רק שהגיבוי הזה היה על מחשב ברשת. וברגע שהתוקף הצפין את המחשבים הוא גם הצפין את הגיבוי. זאת אומרת, לצורך העניין, הם נותרו בלי גיבוי. צריך להיות... צריך להבין שצריכים כאן התייחסות מאוד זהירה, כשבעצם לוקח לאנשים הרבה זמן להבין בעצם שהתשתית הקריטית שלהם, תשתית המחשוב, כרגע מאוימת. והיא מחייבת התייחסות אחרת ממה שהיתה עד השנים האחרונות. אני חושב שאנחנו ממש עכשיו באמצע התהליך, זאת אומרת, לצורך העניין, המנהלנים שדואגים לזה שיהיה אבטחת מידע יותר טובה בישראל כרגע זה חברות הכופרה.

יובל: מה מידת ההצלחה של התקיפות האלה, על כל עשר תקיפות, או על כל מאה תקיפות, כמה הופכת להיות תקיפה מוצלחת?

בועז: תקיפה מוצלחת זה אומר שבסוף הם מקבלים כסף הפושעים?

יובל: לא, תקיפה מוצלחת זה אומר שהצלחתי באמת להצפין לך את המידע.

בועז: אני חושב שאחוזים מאוד גבוהים, אני חושב שבסביבות חמישים אחוז מהחברות, מצליחים לחדור אליהם ולעשות שם מה שרוצים.

יובל: וואו... ואתה אומר יש עשרות כאלה, זאת אומרת יש עשרות מתקפות שנגמרות בזה שמרימים טלפון או שולחים מייל לחברה

ואומרים להם, חברים, כל המידע שלכם מוצפן. זה מה שאתה אומר?

בועז: כן. ואני אומר שזה די נורא. כי כשמתקשרים אלי ואני שומע את הבן אדם מעבר לקו, אני בעצם מבין בשנייה הראשונה שהגיע אלי עוד נפגע טרור. ושהוא רוצה כרגע רחמים ועזרה. וזה האמת, מאוד מדכא. הכי מדכא זה שתמיד מתקשרים אלי ביום שישי בערב. כאילו.. ב-ראבק, תן לאכול ביום שישי בערב. עזוב אותך מהשטויות שלך. אבל אה... אנחנו עוזרים. אנחנו מסייעים והאמת שזה לא רק אנחנו. יש בישראל היום המון חברות. רוב החברות היום עוזרות בסיוע בהתאוששות בתקיפות סייבר. ומנסות לייצר גם אחרי זה מערך סייבר, מערך הגנה יותר טוב.

יובל: אבל העצה שלך באופן מדהים, אל תשלמו.

בועז: העצה שלי אומרת, אם אתה, יש לך מערך גיבוי קודם כל נורמלי, אז אין שום סיבה שתשלם. והדבר השני הוא שמה שראינו שבמרבית המקרים, אם יש לך לצורך העניין בסיס נתונים גדול שהוצפן, בדרך כלל ההצפנה מתבצעת מאוד מהר והיא בעצם מתבצעת בתהליך שנקרא quick and dirty בדרך כלל הקובץ עצמו נפגע במהלך תהליך ההצפנה. והתוצאה היא שבסוף אתה, גם אם אתה תקבל את המפתח והכל טוב ונקי ויפה, כשתעשה את תהליך השחרור, אתה תגלה בעצם שהקובץ נפגע או פגוע ויהיה לך מאוד קשה להתאושש. לכן צריך מאוד להיזהר עם ההחלטה מתי משלמים. אבל יש עוד משהו שאני רוצה להזהיר, אם אתה פותח את ההצפנה בלי שהבנת איך חדרו אליך לחברה, לצורך העניין, האם זה נעשה במייל? האם זה נעשה בחולשה בשרת האינטרנט

שלך? ולא מצאת את המקום שממנו נכנסו ועשו את הפעולה, תהיה בטוח, בצורה... הייתי קורא לזה אבסולוטית, שבעוד מספר שבועות, כל התהליך הזה יחזור על עצמו שנית. או שלישית, או רביעית. ובדרום אמריקה ראינו חברה לאחרונה שהוצפנה שש פעמים במהלך השנה האחרונה.

יובל: שש?

בועז: שש. וכל פעם היא שילמה את כל הכופר מחדש.

יובל: באילו סכומים מדובר? רק שיהיה לנו סדר גודל.

בועז: אז פה באמת יש שונות מאוד גדולה. אם התקיפה היא מה שאנחנו קוראים תקיפת רסס, לצורך העניין, מנסים לשלוח להרבה מאוד חברות ומה שיצליח יצליח. בדרך כלל התשלום יכול לנוע בין... בסביבות מאות דולרים. אם התקיפה היא תקיפה שהכינו אותם אנשים מאוד... נקרא לזה רציניים, אספו מודיעין, הבינו איך החברה בנויה. בודקים את המאזן שלה, בודקים את האנשים שמתפעלים אותה וזה, אז זה יכול להגיע למיליוני דולרים. התקיפה האחרונה שראינו על חברת טאו סמיקונדקטורס, אין לי מושג מה נאמר, אבל לפחות מפרסומים שונים מדובר על כופר של מיליוני דולרים. זאת אומרת לצורך העניין אנחנו במשרע מאוד גדול של תשלום.

יובל: בלוק, מרכז הגנת סייבר לאזרחים הוא מיזם שהקים איגוד האינטרנט הישראלי לרווחתם של בעלי עסקים קטנים ואזרחים פרטיים, בכתובת: www.block.org.il אפשר לקבל טיפים, המלצות ומענה ממוחי סייבר במקרים שבהם יש חשש מהתקפה, או חשש מפני תקיפה עתידית. אנחנו עוד נשוב ונדבר על בלוק ועל

הדרכים להתגונן, אבל לפני כן בועז, בוא ננסה להבין את הצד התוקף. מי הם הגורמים שמנסים לתקוף את האדם הפרטי?

בועז: אז בגדול היום מי שעושה את התקיפות, יכול להיותש זה בדיוק אותם גורמים שראינו ודיברנו עליהם קודם. לצורך העניין, מדינה שבעבר ניסתה נגיד לחדור לתוך חברה, דרך מערכי המחשב שלה, בוחרת היום לחדור ליובל דרור ישירות למחשב האישי שלו, או לבועז דולב ישירות למחשב האישי שלו, שמחובר בבית לראוטר שאולי הוא לא מאובטח, של חברת בזק. עם סיסמא שהיא אותה סיסמא לכולם. וברגע שנכנסו פנימה יש להם בעצם אולי גישה למייל של אותו בן אדם. ואולי למייל הארגוני. ואולי הוא מתחבר דרך המחשב האישי שלו בבית לחברה, אז הם יכולים עכשיו לחדור לחברה דרך המחשב האישי. זאת אומרת, אז אנחנו רואים בעצם שגורמים שהם ממש גורמים מדינתיים, לצורך העניין, התקיפות האחרונות של הצפון קוריאנים, תקיפות אחרונות של האיראנים, תקיפות אחרונות של הרוסים, היתה על ידי זה שניסו בעצם לחדור למחשב האישי שלך בבית. לא כל כך התעסקו במערכי ההגנה הארגוניים, כי יודעים שזה מאוד קשה. ולכן עושים כאן עקיפה. עקיפה שהמטרה שלה זה להגיע למידע הארגוני דרכך. זאת אומרת, אתה לצורך העניין משמש כפרוקסי. אבל חוץ מזה יש כמובן פושעים שהמטרה שלהם זה לגנוב מידע וידע ואולי לאיים עליך. ואולי אפילו לסחוט אותך על ידי זה שתקבל משהו מאוד נחמד שאומר, אחי ראיתי אותך מסתכל במסך בפורנהאב ועושה כל מני דברים. תשלם בבקשה כסף. זאת אומרת, אנחנו מדברים כאן על הרבה מאוד גופים כשנוספים כאן

גם באמת גם פושעים קטנים שמנסים להגיע אליך הביתה, כי הם לא מתעסקים בכלל בחברות גדולות.

יובל: אני רוצה להבין האם אנחנו מקבלים הגנה ממישהו. זאת אומרת, האם מישהו עוזר לנו? או שאנחנו לבד במערה הזאת לגמרי? למשל, האם המדינה מספקת לי, האזרח, איזה שהיא שכבת הגנה?

בועז: תראה, התשובה היא קצת מורכבת, אבל תשעים אחוז התשובה היא לא. זאת אומרת, לצורך העניין, ברוב המקרים אין לך בעצם שום מעטה הגנה. אתה צריך בעצם לעשות מה שנקרא, את ההגנה הבסיסית. זה כמו כשאתה בבית היום, אז יש לך דלת שיש עליה מנעול ואולי יש לך סורגים ואולי גם יש לך אזעקה. אתה שומר בעצם באופן בסיסי על הנכסים האישיים שלך. גם במחשב שלנו. גם המחשב שלנו הוא הנכס האישי. אמנם במקום וירטואלי יחסית, שאתה חייב לשמור עליו. הרצון כמובן... אני גם לא יודע, תקשיב, יובל, יש כאן גם דברים אחרים. החדירה לפרטיות... כי אם המדינה תבוא ותגיד, תקשיב אחי, אני שומר עליך, תעביר את הכל דרכנו, אנחנו עכשיו נהיה הפרוקסי שלך, יכול להיות שאתה בכלל לא רוצה שזה יקרה, יכול להיות שאתה אומר, תקשיבו, אני צריך את החופש שלי. אני רוצה להרגיש ככה והתמורה לזה היא בעצם שאתה מסתכן יותר. וזה כמו שאתה יוצא לטיול בחוץ לארץ, אתה לא תרצה שמדינת ישראל תשלח איתך שומר ראש לכל מקום. שזה פחות או יותר מה שקורא באינטרנט, אתה הרי משוטט בכל העולם. ולא מעניין אותך שהשב"כ ישלח יחד איתך שומר וגם תצטרך לתת לו ללכת לשירותים כשהוא צריך.

יובל: אז אם אנחנו מסתכלים, אז הבנו, אז יש לנו פושעים, יש לנו ארגוני פשיעה, יש לנו מדינות. יש לנו כל מני סקריפט קידיס, לא משנה. מה הן השיטות המרכזיות, ככה כשאתה מנסה למפות אותן, מה הן השיטות המרכזיות שבהן אדם פשוט מן השורה, הוא לא עובד ברפא"ל. הוא לא עובד בתעשייה האווירית. מה הן השיטות המרכזיות שבהן מנסים לתקוף אותו?

בועז: אני חושב שהשיטה המרכזית היא באמצעות מייל. זאת אומרת, לצורך העניין, תקבל דבר דואר שיש שמה איזה שהוא ניסיון לשכנע אותך, או באמצעים של נקרא לזה הונאה או הנדסה חברתית. או על ידי זה ששולחים לך איזה שהיא... איזה שהוא קובץ שבעצם חושף או משתמש באיזה שהיא חולשה במערכת המחשב שלך. ודרך הדבר הזה להיכנס לתוך המחשב שלך ולהשתלט עליו. ואחרי זה לעשות כל מני דברים. אבל אנחנו רואים שבמהלך השנה וחצי האחרונות יש עוד הרבה מאוד שיטות שמשתמשים בהן. לצורך העניין, משתלטים לך על הנתב הביתי ודרך הנתב הביתי נכנסים לתוך המערכות שלך. נפגשים איתך בפייסבוק, נפגשים איתך בלינקדאין ואומרים לך תקשיב, אנחנו רואים בפייסבוק, יש קמפיין מדהים של החמאס. והוא כבר שלוש שנים כל הזמן יוצר בפייסבוק דמויות של בחורות מדהימות, צעירות, חתיכות, תל אביביות. שמנסות לפתות חיילים. אחי, אני חברה שלך, בוא נהיה חברים. בוא זה... תמונות מקסימות. ואז חיילים נהיים חברים של ה... דמויות הפייקיות האלה. ואז הם שולחים איזה שהוא קובץ, אולי דרך מסנג'ר או משהו אחר, שבעצם עוקף את כל המנגנונים ואולי אפילו יורד בטלפון. ודרך זה

הם משתלטים לך בעצם על הטלפון, על הסלולר. שזה עוד משהו שהוא בעצם דרך. זאת אומרת, אנחנו רואים שזה כל הזמן זז קדימה. השיטות זזות בהתאם לאמצעים שבהם יש את המשתמשים. לצורך העניין, אנחנו משתמשים במכשיר סלולרי, מנסים להשתלט לך על הסלולרי. תלוי גם באינטרס של התוקף.

יובל: אבל זה בעיקר, ממה שאתה מתאר, הנדסה חברתית. כלומר, ניסיון לשכנע אותך לגעת באיזה שהוא משהו שהוא נגוע.

בועז: אז זה תלוי. לצורך העניין, נגיד שהחמאס יודע לעבוד בהנדסה חברתית. אבל חברת NSO יכולה להשתלט לך על הטלפון בלי שאתה עושה שום דבר. סתם קיבלת הודעת ווטסאפ... סתם אני נותן דוגמא על NSO, בוא לא נתעלל בחברה. החברה מדהימה. היא מייצאת בהרבה מאוד כסף. מכניסה הרבה כסף למדינת ישראל. אבל אנחנו מדברים כאן על זה שבעצם יש היום חולשות. מה שנקרא zero days, שדרכם אתה יכול בעצם בלי שבן אדם התבקש לעשות משהו בעצם להשתלט על ה... או על המחשב שלו, או על הטלפון. או על הסלולרי שלו. ובעצם זה עוד תהליך שמתנהל, כשבעצם קשה לך מאוד לשלוט בתהליך הזה. אתה לא יודע בתור יובל, או אני בתור בועז אם עכשיו השתלטו לך על המחשב, כי פשוט ניצלו סוג של חולשה שכרגע אנחנו לא יודעים עליה ואז יהיה לנו מאוד קשה לראות שמישהו באמת חדר לנו למערכות שלנו.

יובל: לפעמים הניסיונות האלה הם הרבה יותר איזוטריים. לפעמים הם מנסים להגיע אליך דרך השואב אבק הרובוטי שלך, עד כדי כך?

בועז: כן. אז תראה, קודם כל אין לי שואב אבק רובוטי.

יובל: בגלל זה? זו הסיבה?

בועז: לא, זאת לא הסיבה. אני לא מפחד מ... להפך, אני ממש מת על גאדג'טים, אבל באמת אנחנו רואים שיש הרבה מאוד כלים, לצורך העניין, כמו מה שנקרא מוצרי מבוססי תקשורת. לצורך העניין, מקררים והיום מזגנים וכל דבר אחר שבעצם אתה... הם הופכים להיות לסוג של מחשב. הם יכולים בעצם לשמש כבסיס לתקיפה. לצורך העניין, מכשירי... מכשירים מהסוג הזה לפעמים משתלטים עליהם ומייצרים דרכם תקיפות DDOS תקיפות מניעת שירות, שבעצם מייצרים הפסקת עבודה לאתרים מאוד גדולים בעולם. אבל גם אם אפשר לחדור אליהם ודרכם להאזין לך, לצורך העניין ראינו באמת קומקומים שהגיעו מסין ושבהם יש סוג של אה... צ'יפים שלא צריכים להיות שמה, בוא נגדיר את זה ככה.

יובל: קומקומים מסין?

בועז: כן, קומקומים מסין. אנחנו מתקדמים עם זה לכל מקום שתרצה, זאת אומרת, לצורך העניין, ברור לחלוטין שמכשירי החשמל שלנו בשנים הקרובות הופכים להיות חלק מרשת האינטרנט, הם מתחברים לאינטרנט. הם יגידו לך אם יש מספיק מים במקרר, אם יש מספיק מים בקומקום, אם יש... אם אני צריך לקנות עוד דברים במקרר. ובעצם אנחנו חושפים בעצם במובן מסוים, זה שאנחנו הופכים להיות סוג של מקושרים בכל דבר, בעצם מצד שני אנחנו חושפים את עצמנו לכל תקיפה אפשרית באמצעים או במוצרים שבעבר לא חשבנו בכלל שאפשר לתקוף דרכם.

יובל: מה זה sim swapping?

בועז: סים סוופינג זה תהליך מאוד נחמד. שבו בעצם משתלטים לך על מכשיר הסלולר שלך. משתלטים על מכשיר הסלולר, זה תהליך מאוד כואב. בארצות הברית למשל, מרבית הארנקים של הכסף הדיגיטלי, או הקריפטוגרפי, נגנב על ידי זה שעשו תהליך של סים סוופינג. וברגע שהשתלטו כביכול על הטלפון שלך, שהוא בעצם המזהה שלך, היה אפשר לצורך העניין לעשות ריסט לסיסמת הארנק הקריפטוגרפי שלך ולגנוב המון כסף. אם נגיד אתה מייצר כרגע מצב שאתה נכנס לג'יימייל, אוקיי? לתיבת הדואר האלקטרוני שלך ואתה אומר, עכשיו אני גם רוצה שכשמישהו רוצה להחליף אצלי סיסמא לקבל הודעת SMS שבה כתוב, אנא תכתוב את הקוד 345... סליחה, 432, לא משנה. ואז תוכל להחליף סיסמא. אם השתלטו לך כרגע על המספר הסלולרי שלך, בעצם כשמישהו מרסט או מנסה להחליף סיסמא, הוא יקבל גם את הקוד הזה שצריך להזין אותו. ובעצם הוא ישתלט לך עכשיו על החיים הדיגיטליים. הסים סוופינג יכול להיעשות על ידי זה שלמשל אתה מתקשר לחברת הסלולר במקום בן אדם מסוים ואומר, אחי, תקשיב, יש לי טלפון חדש. בבקשה תעביר את המספר לטלפון הזה. ואתה נותן את המספר או את המזהה הפיזי של הסלולר. ובעצם עושים לך העברה.

יובל: מהרגע שמשתלטים על החשבון, מהרגע שאני יכול למשל לעקוב אחר הרגלי הגלישה שלך, בעצם אפשר ממש לייצר תביעת אצבע

דיגיטלית ייחודית לך, נכון? סיפרת לי על איזה שהוא מחקר כזה של מוזילה.

בועז: כן, יצא עכשיו מחקר של מוזילה, שמדבר על זה שאם אתה מקבל את המאה חמישים הגלישות האחרונות שלך, את ההיסטוריה של הגלישה שלך, אתה בעצם יכול לייצר מצב שמחר בבוקר, לא משנה מאיזה פלטפורמה מישהו יגלוש אתה תוכל להגיד זה בועז, כי ראיתי שהוא גולש קודם כל לדה מרקר, אולי למעריב, אולי אחרי זה ל... לא יודע מה. ישראל היום.

יובל: זה עד כדי כך ייחודי שזה מייצר תביעת אצבע ייחודית?

בועז: כן. זה מייצר תביעת אצבע ייחודית. ואפשר יחסית מאוד בבירור לזהות בן אדם על ידי זה שאתה בעצם חשוף לצורך העניין למשהו שהוא לכאורה לא מזהה שום דבר, או לצורך העניין אנונימי לחלוטין. לכן, לצורך העניין, אם גוגל מוכרת את הרגלי הגלישה שלך למישהו, גם זה יכול לייצר מצב שבו מבינים או מייצרים סוג של תביעת אצבע אליך. וזה מאוד מסוכן. הפרטיות שלנו ממש בזבל כרגע.

יובל: כשאתה מסתובב בפורומים, ואתה מסתובב בפורומים שבהם מוכרים מידע על גולשים, מה מוכרים? ומי קונה?

בועז: אז תראה, האמת שהיום בבוקר לפני הישיבה שלנו, לפני הדיון שלנו, אז הסתכלתי מה קורה בפורום נחמד שבו מוכרים פרטים של אנשים מכל העולם. וצריך להבין שיש פורומים שבהם כל פרטי הה זדהות שלנו נגנבים. אני מעריך שבין עשרות למאות אזרחים נגנבים פרטי ההזדהות שלהם בכל יום ומוצעים למכירה במחירים יחסית מצחיקים. מה זה מצחיקים? בסביבות עשרים דולר לבן

אדם בדארק נט. היום בבוקר ראיתי בן אדם שמפורסם, תמורת 28 דולר אתה יכול לקנות את 302 הסיסמאות שלו לאתרים שהוא גולש בהם וגלש בהם. וכל חייו בשנה האחרונה. אני אגיד לך דוגמא כי פשוט יש לי אותה מול העיניים. אז אתה יכול לקבל את הסיסמא שלו לגוגל, לאיביי, לאמזון, למסנג׳ר, לפייסבוק. לטוויטר, לאדובי, ללינקדאין. לאינסטגרם, לנטפליקס, לוויקיפדיה, לפייפאל. לאורנג׳, לבנק לאומי. לבנק מזרחי טפחות. אה... לאן? לא משנה, אני אגיד, לבזק. ויש לך בעצם את כל החיים הדיגיטליים, בעצם נגנבים מאנשים בכל יום.

יובל: מי קונה את המידע הזה? אתה עושה את זה כתחביב. אבל מי... מי קונה? מי הם הלקוחות של האינפורמציה הזאת?

בועז: אז קודם כל אני לא עושה את זה כתחביב, יש לי חברת סייבר. ואם אני מזהה שכרגע יש נגיד מישהו שהפרטים שלו בכניסה לאחד מחשבונות הבנק של הלקוחות שלנו, פתוחים, אז אנחנו קונים את המידע רק בשביל להתקשר לאותו בן אדם ולבקש ממנו להחליף סיסמאות. אבל יש הרבה מאוד גורמים, מגורמי תקיפה מדינתיים ועד גורמי פשיעה, שברגע שהם גונבים את הנתונים האלה, מבחינתם הם יכולים להיכנס לכל הנכסים שלך ולעשות כמעט כל מה שהם רוצים ולכן, כולם קונים, גם הטובים, גם הרעים. כל אחד מהסיבות שלו, אבל בסוף מי שאוכל אותה, זה אנחנו.

יובל: איך נשמעת ונראית שיחה שבה אתה מרים טלפון לאדם ואומר לו, אדוני, אני לפני רגע הייתי בפורום ורכשתי את הפרטים שלך. נפרצת. איך... איך זה נראה?

בועז: לפני שבוע, ממש לפני שבוע, בשבוע שעבר, משרד רואי חשבון גדול בישראל, ראינו שבעצם נפרץ. נפרץ על ידי דווקא האיראנים. והתקשרתי לרואה חשבון שהוא בעצם המנהל של המשרד ואמרתי לו שלום, שמי בועז דולב, אני מחברת קליר סקיי. רציתי להגיד לך שבעצם המחשבים שלך פרוצים. אתה מבין שבצד השני יש בן אדם שמרגע שאמרת לו את זה, הוא מיד חושב ש-א', באת לסחוט אותו. ו-ב' שאתה בעצם מנסה לעבוד עליו או לא יודע מה. ולכן התגובות מאוד לא טובות. ולכן אני מאוד מסתייג בכלל מלעשות את השיחות האלה. בדרך כלל אני מעביר את המידע הזה לגופים שהם כמו בנקים, אולי מערך הסייבר ואומר להם, תקשיבו, תתקשרו אתם. אני, כשאני מתקשר, מידת עוגמת הנפש שאני גורם לאנשים וגם חוסר האמון, מבחינתי זה לא משהו ששווה בכלל את הטלפון הזה. וזה מאוד קשה. זה מאוד קשה לשמוע אנשים שבעצם נפגעו. ואנשים שגם לא מבינים מה הם צריכים לעשות, זאת אומרת, אתה צריך גם להסביר לו, תקשיב, אתה צריך להחליף עכשיו את כל השלוש מאות סיסמאות שלך. בן אדם לא יודע על מה אני מדבר. הוא אפילו לא יודע שיש לו שלוש מאות סיסמאות. אז גנבו לו בעצם את הפסוורד מתוך גוגל, מתוך כרום או משהו כזה. אבל הוא לא זוכר אפילו איזה גופים או איזה סיסמאות הוא נתן בכל אחד מהדברים האלה. לכן זה אירוע מאוד קשה. כמעט חודרני. זה חדירה לפרטיות מטורפת. עכשיו, אם הבן אדם גם גולש באתרי פורנו ויש את הסיסמאות שלו מולי. אז אני גם חשוף גם בעצם לדברים הכי אינטימיים שלו. ולכן זה מאוד מורכב הדבר זה.

יובל: אני בטוח שבשלב הזה, אחרי הסקירה הקצרה אבל הדי ממצה הזו, המאזינים אומרים לעצמם, אוקי, שוכנעתי. אני צריך להגן על עצמי ואני שוחחתי איתך על העניין הזה. ואמרתי לך, אוקי, אז איך אני מגן על עצמי? ואתה אמרת לי, אין דרך להתגונן. תסביר.

בועז: התשובה היא כן, קשה מאוד להתגונן מפני דברים שאתה, לצורך העניין מפני חולשות. זירו דיי ואחרות. אתה לא תוכל להגן. אבל אם אתה שומר לצורך העניין על זה שסיסמאות הן מה שנקרא עם אותנטיקציה כפולה. לצורך העניין אתה מקבל סיסמא, אבל אתה חייב להוסיף עוד איזה שהוא מזהה. אם אתה עובד עם גוגל אותנטיקייטור, סוג שאתה מקבל סיסמא זמנית מתוך הסלולר. אם אתה מקבל הודעת SMS, כל דבר שבעצם יחזק את היכולת שלך להגן על הסיסמאות שלך. כמובן שתבחר איזה שהיא סיסמא נורמלית על הדברים האלה. וגם זה נשמע גרוע, כי זה מאוד קשה, כי אם עושים עליך לצורך העניין מבצע של הנדסה חברתית, יהיה לך מאוד קשה, בהנחה שהם מבינים איך אתה, את הדברים שאתה אוהב, ואיך אפשר להגיע אליך. אז יהיה לך קשה להתגונן מפני סוג כזה של תקיפה. ולכן האתגר הוא כאן ענק. אנחנו נמצאים היום בתקופה שבה בעצם התוקפים הם בסדר גודל מצליחים לעומת היכולת שלנו להגן ולכן באמת התהליך הוא מאוד קשה. והוא כרגע גם מאוד כואב להרבה אנשים. הרבה מאוד אנשים.

יובל: ובכל זאת אתה לא אומר אל תעשו כלום. ואני שואל אותך, מה העצה שלך אלי? המאזין הפשוט. איזה VPN להתקין? איזה אנטי

וירוס להתקין? מה בכל זאת אתה אומר למשתמש הרגיל בניהול הסיכונים? אלה הם הכלים הטכנולוגיים שבהם אתם צריכים להשתמש.

בועז: תראה, באופן עקרוני, אל תיקח אנטי וירוס שהוא חינמי. מצטער כאילו... רגע, סליחה, אני אסתייג. האנטי וירוס של מייקרוסופט שמגיע עם מערכת ההפעלה, היא יחסית מאוד טובה. הוא מאוד טוב. אפשר להשתמש רק בו אבל להקפיד שהדיפנדר מותק ושהוא עובד ושהוא מקבל עדכונים. בהנחה שאתם רוצים עוד משהו מעבר לזה, אז ESET וקספרסקי וכל שאר האנטי וירוסים, טרנד מיקרו ואחרים, דורשים תשלום של בין עשרות למאות שקלים. לדעתי עשרות שקלים לשנה. ואני ממש ממליץ להתקין אותם. הם עושים עבודה טובה מאוד. פרט לזה כמובן אני הייתי מייצר לעצמי איזה שהוא סוג של גיבוי. לצורך העניין לקנות, להשקיע בדיסק. אחת לחודש לחבר אותו למחשב. ובעצם לגבות את המידע, כדי שאני אוכל לדעת שלפחות חודש אחורה אני אוכל לקבל את הנתונים. אז זה שני הדברים הקריטיים של זה. וכמובן לדאוג לזה שהמחשב שלי, לצורך העניין, המערכת הפעלה מעודכנת, מקבלת עדכוני אבטחה כמו שצריך. וזה אני חושב אחד מהדברים החשובים. לדאוג לזה שתמיד המערכת מעודכנת. כי אז הרבה מאוד איומים שבעצם מתגלים נחסמים על ידי החברות היום. וזהו. ובסוף כמובן אפשר להתפלל, כל אחד לאל שלו ואיך שהוא חושב שהכי טוב לו להתפלל זה מצוין.

יובל: נשמע אופטימי. כרגיל. אחד הפתרונות שבכל זאת מוצעים לגולשים רגילים נקרא בלוק. זה פתרון שאותו פיתח איגוד האינטרנט הישראלי. היית מעורב בו. ספר לי רגע עליו.

בועז: אני אספר. תראה, באיגוד האינטרנט הישראלי עושים עבודה שהיא די מדהימה. ומנסים בעצם לסייע לאזרחים להתמודד עם תקיפות סייבר. במסגרת הזאת הוקם בעצם האתר block.org.il, אפשר גם להיכנס לאתר של איגוד האינטרנט הישראלי ולהגיע משם. ושבעצם אנשים מוזמנים שם להעלות שאלות או סוגיות שבהן הם נתקלו. ויש אנשים באיגוד האינטרנט, או מטעם איגוד האינטרנט, או מטעם קהיליית אנשי אבטחת המידע, שהם בעצם מסייעים. לצורך העניין, אם באמת קרה לך משהו, המחשב שלך נתקע, יש לך חשש שהותקפת בווירוס ואתה הוצפנת או משהו כזה. להיכנס לשם ולהגיד, תקשיבו, זה מה שקרה לי. ויהיה איש מקצוע שיענה לך ויסייע לך ויגיד לך מה בעצם צריך לעשות. אולי הוא יפנה אותך לאנשים אחרים. אולי הוא יפנה אותך למידע שכבר קיים לגבי איך מטפלים בתקיפות. אבל בסך הכל זה אוזן קשבת לאזרח, כמעט 24 כפול 7. וזה מקום מאוד מעניין לקבל ממנו עזרה ראשונית.

יובל: עוד שאלה לי אליך, דיברנו על חדירה לפרטיות ומה אפשר ללמוד בעצם לייצר תביעת רגל, אצבע, דיגיטלית עליך, אבל זה לא רק שממש חודרים לך למחשב. כשאתה יורד מירושלים לתל אביב, למקום העבודה שלך, עד כמה פרטיות יש לך רק במסע הזה?

בועז: קודם כל אני מאוד שמח יובל שנזכרת שאני כל בוקר נוסע מירושלים לתל אביב. אבל התשובה לזה היא תהיה מאוד רצינית,

כי אני רוצה שתבין שבבוקר, כשאני קם בבוקר ונוסע עכשיו לעבודה, אני בעצם לוקח איתי אצטדיון שלם של אנשים. ואני אנסה פשוט להגיד לך איך זה קורה. אז קודם כל אני נמצא עם המרגל האישי שלי.

יובל: הטלפון שלך.

בועז: נכון. ואליו נגיע בהמשך. אבל כשאני מניע כרגע את האוטו, אז יש כמובן איזה שהיא חברה אחת או שתיים, למשל פוויינטר, שעוקבת אחרי הרכב שלי לצורך מניעת גניבות. והם יודעים בכל שלב איפה אני נמצא. לצורך העניין, אני מקבל הודעות, הודעות SMS כמו, לקוח פוויינטר יקר, זוהתה התנעה לא שגרתית ברכב, במידה ובוצעה ללא הסכמתך, אנא התקשר אלינו בדחיפות. או, רכב נקלט בשעה מסוימת בנסיעה באזור יהודה ושומרון, במידה והנסיעה אינה מתוכננת, אנא התקשר אלינו מיד, עם המבצעים. זאת אומרת, לצורך העניין, אני לוקח עכשיו את החבר'ה של פוויינטר איתי לכל מקום. אחרי זה, אם אני נגיד נוסע בתחבורה הציבורית, רחמנא ליצלן, אז ברגע שהעברתי את כרטיס רב קו באגד או בדן או בכל חברה אחרת, זהו, אני כבר יודעים בדיוק שעליתי לאוטובוס. עכשיו נכנסתי לרכבת ישראל, העברתי את רב קו, זהו, יודעים שעליתי לרכבת, גם יודעים לאן. ואם הזמנתי את גט טקסי, ברגע שעשיתי את זה, אני כרגע באפליקציה שלהם והם יודעים בדיוק לאן אני נוסע. עכשיו נעבור הלאה. אתה נוסע בכביש, אתה בנתיבי ישראל, לצורך העניין מע"צ לשעבר. יש להם מצלמות בכל מקום. מצלמים אותך. אתה יכול להיות במצב שרואים אותך מכל מקום. הם פרסו עד עכשיו מאות מצלמות,

אבל בעיקרון אתה יכול אפילו להיכנס לאינטרנט ולראות איפה עכשיו בועז נמצא. אחרי זה, נגיד שתדלקת, או עצרת לקפה, או הוצאת כסף ממכשיר בנק אוטומטי. אז חברת הדלק והתחנה שבה עצרתי, כמובן היא יודעת, כמובן המצלמות שלה יודעות שעצרתי. בית הקפה, המצלמות בבית הקפה, חברת ה-ATM שממנה הוצאתי כסף, המצלמות של מכשירי ה-ATM, כולם צילמו אותי, אז כבר הגענו למצב שיש בערך מאה אנשים בבוקר שיודעים שעכשיו אני בדרך מרושלים לתל אביב. אבל בוא נמשיך הלאה, חברת כרטיסי האשראי, ברגע שעשיתי טרנסאקציה שמבוססת כרטיס אשראי, קניתי עכשיו קפה בקפה 443, הקפה האהוב עלי. הדרך אל האושר. אז הם יודעים שעכשיו אני קניתי ב-443 ואני בדרך לתל אביב. עכשיו נגיע למרגל האישי. מכשיר הסלולר. אז כמובן שחברת הסלולר יודעת בכל שלב איפה אני נמצא. היא יש לה את כל האנטנות שמקשרות אותי לעולם. יודעים, עכשיו בועז נמצא באזור א', ב', ג'. ועכשיו נלך לכל החברות שיושבות על המכשיר הסלולרי, לצורך העניין, גוגל, אפל. כל החברות והיישומים שאנחנו מתירים להם לעקוב אחרי המיקום שלנו. כאן כבר הגענו לאלפי אנשים, כולל סינים, כולל רוסים. מאיפה אתה יודע למי גוגל מוכרת בכלל את הנתונים שלך? עכשיו, זה קטע מדהים. עכשיו כמובן לא הזכרתי את ווייז. ווייז הרי אני נוסע איתו כל היום. ווייז מקושר לגוגל, גוגל מקושר לגוגל קסטומרס, גוגל קסטומרס מקושרים לרוסים. אז בעצם אני רק רציתי לספר לך שכשאני נוסע בבוקר מירושלים לתל אביב, נוסע

איתי אצטדיון שלם של אנשים. חלקם לא מכירים אותי. אבל ברגע שהם ירצו הם יכירו אותי. וכיף לי פשוט. אז זה נושא של פרטיות. אז בהקשר של פריצות וזה. לא צריך כבר תמיד לפרוץ, אפשר גם לקנות בסבלנות. מגוגל. ולקבל את כל המידע עלי.

יובל: אחד הדברים שאנשים לפעמים שוכחים, זה שהם מזדהים בהרבה מאוד שירותים באמצעות חשבון הגוגל שלהם. זאת אומרת, כאשר פורצים לך לג׳יימייל, לא רק נכנסו לדואר האלקטרוני שלך. תסביר את הנקודה הזו.

בועז: יש הרבה מאוד פעמים... זו נקודה מצוינת דרך אגב, יובל. הרבה מאוד פעמים כשאתה נכנס לאתר מסוים הוא אומר, אולי אתה רוצה להזדהות באמצעות גוגל עכשיו? ואנחנו בוחרים כמובן להגיד לו, כן אני נותן הרשאה לקבל את המידע מגוגל ותכניס אותי לתוך האתר. זאת אומרת, לצורך העניין, אם גנבו עכשיו את הסיסמא שלך לגוגל, דרך זה הם יכולים להיכנס לכל האתרים שבעצם הענקת להם הרשאה, או שדרכם בעצם נכנסת לאתרים אחרים, זה יכול להיות גם אתרים שהם מאוד כבדים. זה יכול להיות אפילו חברות או ארגונים פיננסיים, זה יכול להיות המון דברים, כי יש היום סוג של החבר שלי הוא החבר של החבר שלי. והחבר של החבר שלי יכול להגיע כאן לדיפננסיס שהם מאוד עמוקים. ושבעצם מייצרים מצב שגניבה של רק הסיסמא שלך היא בעצם, היא אחת, לצורך העניין, גוררת אחריה עשרות סיסמאות לעשרות אתרים אחרים שדרכם אפשר להיכנס עכשיו ולגנוב ממך את המידע.

יובל: זאת אומרת, אם יש נקודה אחת שאנחנו ממש צריכים להגן עליה, זה הגוגל הזה.

בועז: זה הדואר האלקטרוני וההזדהות אליו. זה יכול להיות גם 360 של מייקרוסופט. או גוגל, ג'יימייל. נקודת המפתח של אזרח היום זה בדרך כלל כתובת הדואר האלקטרוני שלו. ועליה צריך להגן מאוד חזק. כמה שיותר ככה יורת טוב, באמת, גם עם מזהה שאולי הגוגל אותנטיקייטר שמותקן על ה... או מייקרוסופט אותנטיתיקייטר, אני לא רוצה להגיד שם כרגע. או אפילו באפל יש להם גם כן איזה שהוא מנגנון של ארנק כזה ששומר את הסיסמאות. קריטי לעשות את זה. להפעיל את זה ולדאוג לזה שזה מנוהל כמו שצריך.

יובל: שתי שאלות אחרונות. האחת, האם מאז 2011 אז הקמת את החברה ועד היום פרצו אליך? הצליחו?

בועז: אני לא ממש יודע. אוקי? זאת אומרת, יכול להיות שגנבו ופרצו ואני לא יודע. וזה ממש מזעזע. אבל היו ניסיונות. היו ניסיונות. האיראנים הקימו לפחות פעם אתר מתחזה לקליר סקיי, כי המטרה היתה לגנוב לקוחות לשם ושמה שנקרא יכנסו לשם וזה. האמת שאני מאוד מוטרד מהעניין הזה. אני חושב שלי ולנו, בסוף, אם מישהו, בוודאי אם זה גורם מדינתי, מנסה לפרוץ אליך, היכולת שלך להתגונן בפניו היא מאוד נמוכה. זה לא שהיא בלתי אפש... זה לא שאי אפשר, אבל באמת הסיכויים להגן הם לא גבוהים. אוקי? כרגע, זה המצב. אני מאוד מקווה שלא. אני לא יודע. אוקי? אבל אני באמת, כל תשובה אחרת תהיה פשוט סוג של התנשאות לא במקום.

יובל: שאלה אחרונה, אתה עוסק בעולם הזה של פריצות ותקיפות ומגננות כבר הרבה מאוד שנים, זה משפיע עליך גם באופן אישי? זה הופך אדם לאדם קצת יותר פרנואידי? שכל הזמן בעצם מתעסק בעולם הזה?

בועז: אני חושב שבגדול אשתי ממש סובלת מזה. לא, באמת, כאילו...

יובל: למה? למה?

בועז: שמתקשר אלי מישהו שעכשיו הצפינו לו את כל החברה. ואני צריך להתעסק עם זה גם בערב, גם בלילה, גם בבוקר. בעצם זה שואב את הזמן שלי וגם את האטנשן שלי ואת היכולת שלי להיות נחמד. ואני חושב שברמה מסוימת זה ממש פגע בי. אני... יש הרבה מאוד פעמים שאני מרגיש ממש שחוק. וזה מאוד קשה, לכן אני כן חושב שזה פוגע במשפחה. וזה מחייב אותי להרבה מאוד, נקרא לזה מאמצים, כדי להמשיך ולעבוד באופן רגיל ומסודר ולהרגיש שבעצם העולם זה לא רק משחקי גניבה וזה. וזה באמת מאוד קשה. בגדול הייתי מאוד שמח לצאת לפנסיה ולהיות עד סוף החיים באיזה שהוא אי מקסים. אבל מצד שני, תראה, אני מאוד אוהב את מה שאני עושה. זאת אומרת, אני ממש אוהב את זה. אני מרגיש שלפעמים אני עוזר לאנשים. לא תמיד. לפעמים אני לא עושה דברים טובים. אבל בסך הכל אני מאוד אוהב את העבודה שלי ואני חושב שהקטע של לאהוב את העבודה זה משהו שהוא מאוד חשוב. וזה אחד הדברים העיקריים שאנחנו בעצם נמצאים כרגע בעולם ויכולים להפיק מהם המון המון, המון דברים טובים. ולכן, בסוף אני רואה את זה כמשהו מאוד חיובי. בדרך זה מאוד קשה.

יובל: בועז דולב, תודה רבה על השיחה המעניינת הזו. עד כאן להפעם, אני דוקטור יובל דרור. ואני מזמין אתכם להצטרף אלינו גם לפרק הבא שיעסוק במופע אחר של חדירה לחיינו. אנחנו נעסוק בקשר ש/בין ריגול, מעקב ודמוקרטיה, נשתמע בפעם הבאה. בכל מה שקשור לאבטחת סייבר לאזרחים, היכנסו ל-block.org.il ואנשי איגוד האינטרנט ישמחו לייעץ, לעזור ולחשוב יחד איתכם כיצד ניתן להגן על המידע שלכם.