

# רפואה מאובטחת

דורון יצחקי, שירותי בריאות כללית: "הפעלת גלישה מאובטחת לעובדים הפחיתה משמעותית את הסיכונים" ♦ "חיפשנו אחר פתרונות של גלישה מאובטחת, שיאפשרו לגולשים חוויית גלישה סבירה וישמרו על ביטחון הרשת, והורדנו את סיכוני זיהום הרשת או השתלטות עוינת עליה", אמר יצחקי, מנהל משאבי תשתיות ושירות באגף המיחשוב של החברה

## יהודה קונפורטס

שהוא מתפרץ ומפעיל את המערכות השונות, בהן האנטי וירוס. "מדובר בקוד מיוחד, שמתאפיין בכך שהוא שומר את המפתח שלו לעצמו, בניגוד ליצרני וירוסים, שמעוניינים להפיץ", הסביר. "הסיבה שהוא שומר אותו לעצמו נובעת מכך שהוא יכול למכור את הקוד הזה במאות אלפי דולרים, לעברייני רשת או לגורמי ביון ומודיעין. הקוד הזה יודע לאתר הרבה קודים חשש לזיהומי רשת ולפעול בהתאם, ולכן יש לו ערך, כל עוד הוא לא נחשף. בשלבים מאוחרים יותר, כאשר כותב הקוד מתחיל לשחררו והוא כבר חשוף, הערך שלו יורד".

הוא ציין כי הפתרון מותקן בארגונים גדולים בישראל, בהם ההגנה נחשבת לקריטית. "אין ספק שבעידן הסייבר יש לפתרונות מהסוג שלנו חשיבות גדולה יותר", אמר גראפי.

דובר אחר בכנס, **מרטין לדהיים**, מנהל תשתיות עמדות קצה במגדל טכנולוגיות, סיפר כיצד הפעלת הגלישה המאובטחת משרתת את מטרות הארגון ובעיקר מאפשרת חוויית גלישה למשתמשי הקבוצה. "כשנכנסנו לתהליך חששנו שנעמוד בפני גידול משמעותי בהיקף המשתמשים שגולשים מחוץ לרשת הארגונית בצורה מאובטחת, עד כדי הצפה", אמר. "עד שהפעלנו את מערך הגלישה המאובטחת, 1,500 משתמשים מתוך 3,000 גלשו באישור שלנו מחוץ לרשת והיו פתוחים לעולם. להפתעתנו, אחרי הפעלת התוכנית, המספר נשאר אותו הדבר, מה שמאפשר לנו לתת שירותי גלישה בטוחים וסבירים לעובדים". לנדהיים ציין כי "לכל גולש יש פרופיל שבאמצעותו אנחנו נותנים לו הרשאות, על פי חוקים שאנחנו מכניסים לתוך מערכות ההפעלה והאפליקציות שמופעלות על ידו".

חתם את האירוע מני צרפתי, מנהל תחום משתמשי הקצה של VMware ישראל. הוא הציג בפני המשתתפים את פתרונות החברה לגלישה מאובטחת, בהם קונספט של שירותי מיקרו-חוץ לארגונים, שמבטיח להם טיפול מאל"ף ועד ת"ו בניהול גלישה מאובטחת ברשת. כן הוא הציג פתרונות של Airwatch, ש-VMware רכשה אותה לא מכבר, והציף בדבריו את סוגיית המובייל ואתגרי האבטחה שלו בארגונים - מה שיצריך בקרוב מאוד פתרון כולל שלם.

הפעלת גלישה מאובטחת לעובדי שירותי בריאות כללית, על כל זרועותיה - בתי החולים, המרפאות והשלוחות האחרות - הפחיתה בצורה משמעותית את הסיכונים לזיהום הרשת שלנו ולהשתלטות עוינת עליה", כך אמר **דורון יצחקי**, מנהל משאבי תשתיות ושירות באגף המיחשוב של החברה.



דורון יצחקי

יצחקי דיבר במפגש של פורום CTO מבית אנשים ומחשבים, שעסק בנושא גלישה מאובטחת ברשת הארגונית. לדבריו, בעבר הלא רחוק, ארגונים מנעו ממרבית המשתמשים שלהם אפשרות לגלוש לאתרים חיצוניים.

"היה ברור לנו שככל שאנחנו פותחים את הגישה לעולם החיצוני, סכנות זיהום הרשת גדלות", אמר. "לכן, חיפשנו אחר פתרונות של גלישה מאובטחת, שיאפשרו לגולשים חוויית גלישה סבירה וישמרו על ביטחון הרשת".

הוא ציין כי אתגרי אבטחת הרשת בכללית מורכבים ביותר, בגלל גיוון המשתמשים וביזורם הרב. "אנחנו מקבלים מדי יום כמיליון אי-מיילים שנשלחו מבחוק, 90% מהם נחסמים על ידי המערכות שמאפשרות גלישה בטוחה", אמר יצחקי. הוא פירט את המרכיבים הטכנולוגיים של הפתרון, שמוצע כשירות מיוחד לכל הלקוחות הפנימיים של שירותי בריאות כללית. "כדי למנוע עומס על הרשת והצפת גולשים על אתרים מסוימים, כל יחידה של הקופה מקבלת תמחיר לשירות הגלישה המאובטחת, שבעזרתה היא מסננת גלישות מיותרות ומאפשרת חלוקת משאבים סבירה לכולם", ציין יצחקי. לדבריו, הפתרון הכללי מורכב מניטור הדואר והמידע שזורם אל הגולשים מחוץ לרשת הארגונית. כמו כן, יש פתרון מבוסס SCOM, פתרון הלבנת רשת, שנועד להגן עליה מפני תקיפות, מבוסס חברת מובייל טיק ומערכת Cockpit למיילים של Jetro Cockpit, המבוססת על תשתית של VMware.

"בסך הכול השגנו חיסכון בעלות החומרה ורישוי תוכנת מערכות הפעלה ב-ADSL, בעלות התקשורת ובנדל"ן", סיכם יצחקי.

## "95% מהמתקפות מגיעות ממיילים"

**אביב גראפי**, ה-CTO של חברת Votiro, הציג את פתרונות הלבנת הרשת של החברה. מדובר בחברה פרטית שהוקמה לפני ארבע שנים על ידי יוצאי יחידות עילית טכנולוגיות בצה"ל. הוא ציין כי "המקור של 95% מהמתקפות על הארגונים, כולל מתקפות סייבר, הוא במיילים שגרמו למשתמשים לחשוף על לינקים ובעקבות זה נפתחה להאקרים הדרך לפרוץ למערכות המידע של הארגון".

גראפי הסביר כי עולם המתקפות פועל על שני תחומים - Malware-1 Exploit. הפתרון של Votiro פועל בתחום ה-Exploit, שם הזירה מצומצמת יותר ואפשר לדעת מראש איזה סוג של קוד נשלח במערכת, לפני

