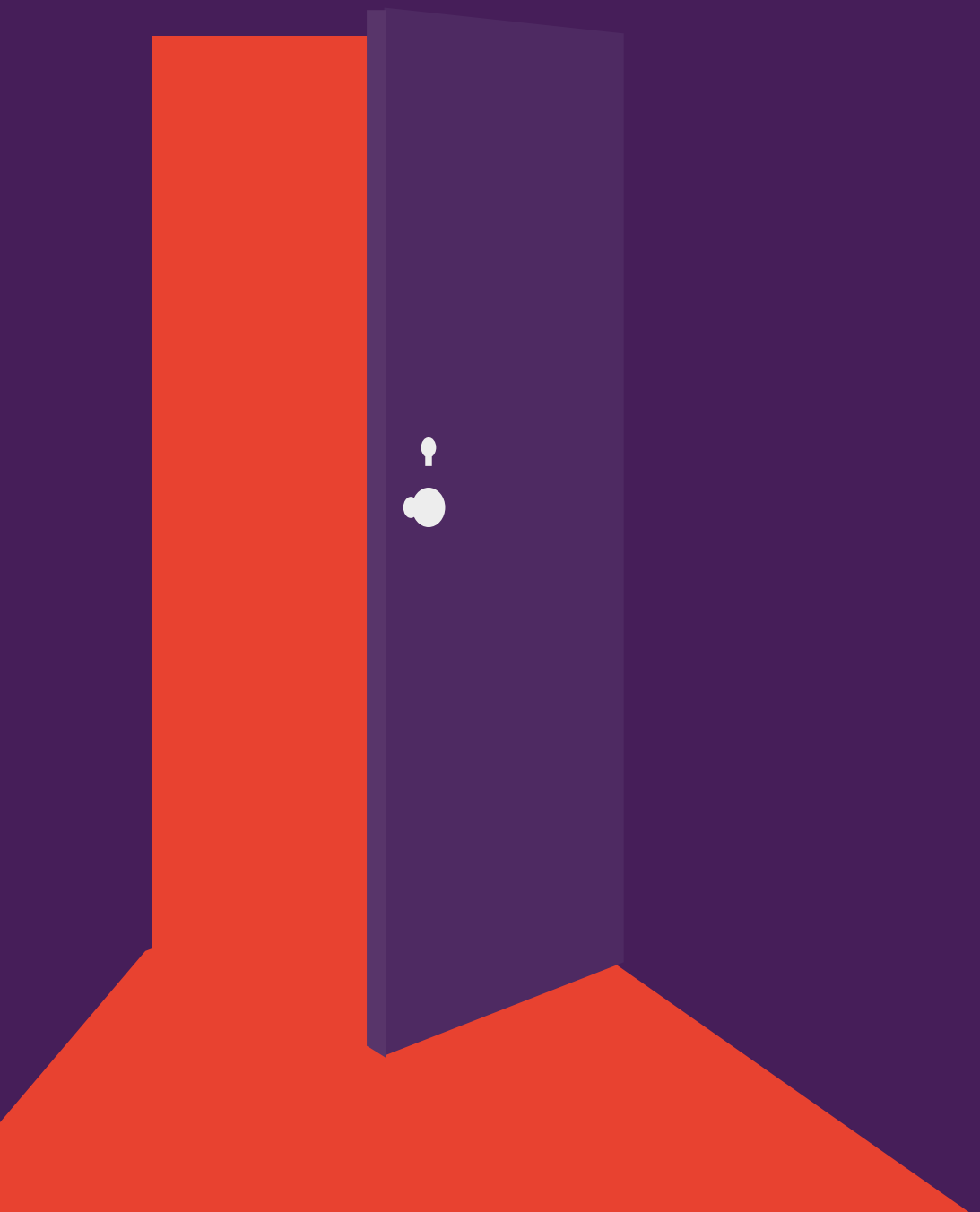
דלתות לא נעולות

מחקרים מראים שמדפסות נשארות פגיעות למתקפות סייבר.

שירותי IT מתמקדים בנקודות קצה אחרות, אך האבטחה של מדפסות ארגוניות נשארת מאחור



מדפסות הן מטרה קלה: ביותר מדי מדפסות המחוברת לרשת אין הגבלות, והן לא נעולות היטב.

אבל האיום אמיתי, ולא כדאי להתעלם ממנו. מדפסות ברמה ארגונית התפתחו והפכו להתקנים מרושתים ורבי עוצמה, עם אותן נקודות התורפה שקיימות בנקודות קצה אחרות ברשת. נקודות הכניסה האלו, שבדרך כלל אינן מוגנות, פותחות אפשרות מוחשית מאוד למתקפות סייבר. בנוסף, הן עלולות לאפשר גישה לנתונים הפרטיים והפיננסיים של החברה, ולהוביל להשלכות עסקיות מוחשיות מאוד.

למרות זאת, לפי סקר שנערך לאחרונה על-ידי Spiceworks, שכלל יותר מ-300 מקבלי החלטות ארגוניים בתחום ה-IT, רק 16% מהמשתתפים סבורים שמדפסות נמצאות בסיכון גבוה לאיומי אבטחה או פריצות אבטחה, אחוז נמוך משמעותית בהשוואה למחשבים שולחניים, מחשבים ניידים ומכשירים ניידים.[1] התפיסה הזו משפיעה על היחס של צוותי IT לנושא אבטחת הרשת. בכמעט שלושה מתוך כל חמישה ארגונים קיימים נוהלי אבטחה מוגדרים עבור מדפסות, אך מדובר באחוז נמוך מאוד בהשוואה לנקודות קצה אחרות - כך שהמדפסות נותרות פגיעות, גם אם קיימים פתרונות פשוטים להגנה על נקודות הכניסה האלו.

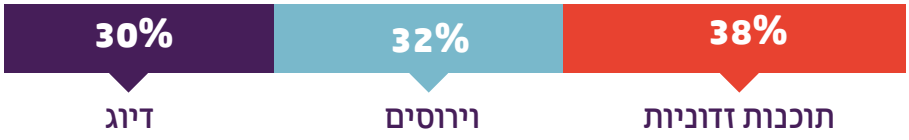
סקירה טכנית זו כוללת נתונים לגבי אבטחת מדפסות על בסיס הסקר של Spiceworks, מידע על ההשפעות של פרצות אבטחה, וסקירה לגבי כמה כמה מהמאפיינים המובנים המודרניים של אבטחת מדפסות שנוצרו כדי להגן מפני מתקפות סייבר.

רק 16% מהמשיבים סבורים שמדפסות נמצאות בסיכון חמור לאיומי אבטחה/פרצות אבטחה.[1]

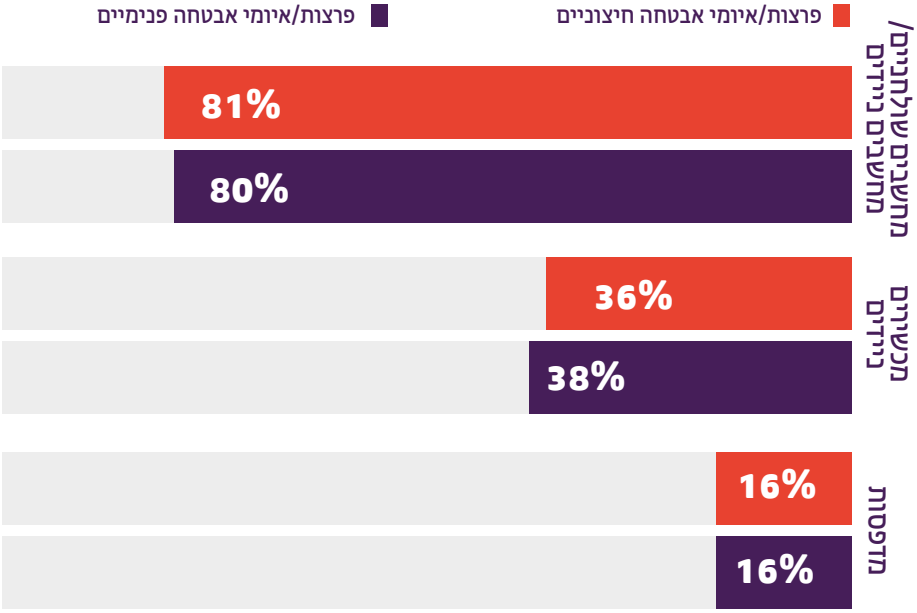
פתחים להתקפה

בסקר של Spiceworks, 74% מהמשיבים (משוקלל) סיפרו שהארגון שלהם חווה סוג כלשהו של פרצת אבטחה או איום אבטחה חיצוניים בתחום ה-IT במהלך השנה האחרונה. בנוסף, 70% (משוקלל) חוו פרצות אבטחה או איומי אבטחה פנימיים בתחום ה-IT, ברוב המקרים כתוצאה משגיאות משתמש, שימוש במכשירים אישיים לצורכי עבודה, או כיוון שעובדים השתמשו ברשת ביתית או ציבורית לצורכי עבודה.[1]

פרצות/איומי אבטחה חיצוניים בתחום ה-IT שהופיעו בתדירות הגבוהה ביותר



האיומים הנפוצים ביותר חדרו בעיקר דרך מחשבים שולחניים וניידים, ואחרים חדרו דרך מכשירים ניידים ומדפסות[1] (ה-16% שחדרו דרך מדפסות מהווים גידול משמעותי בהשוואה ל-4% במחקר דומה של Spiceworks משנת 2014). בנוסף, ייתכן שהאומדן של מספר המתקפות שחודרות דרך מדפסות הוא נמוך מדי, מאחר שניטור המדפסות פחות קפדני מניטור המחשבים האישיים והמכשירים הניידים.



אנחנו מתעלמים מהמדפסות שלנו

בכל מקרה, הסקר של Spiceworks מבהיר שאבטחת מדפסות היא במקרים רבים תחום מוזנח.

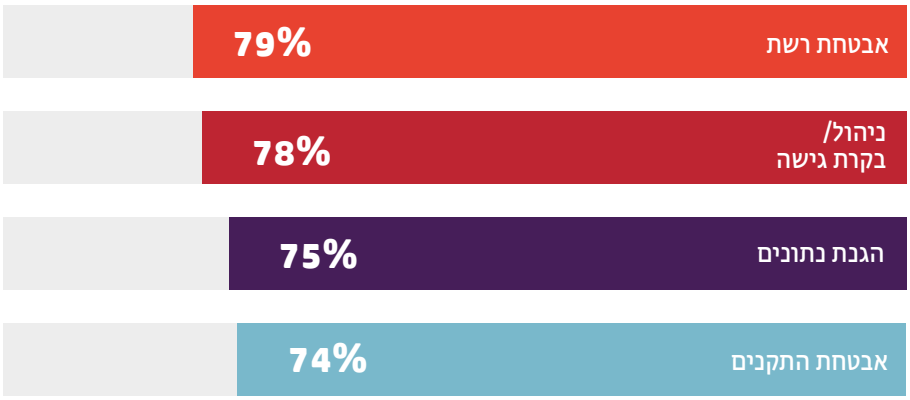
ארגונים מודעים מאוד לחשיבות האבטחה של רשתות, נקודות קצה ונתונים. למעשה, יותר משלושה רבעים מהמשיבים משתמשים באבטחת רשתות, ניהול/בקרת גישה, הגנת נתונים או אבטחת נקודות קצה - או משלבים בין השיטות האלה.[1]

אך כשמדובר במדפסות פריסת הפתרונות האלו היא נדירה הרבה יותר. 83% מהמשיבים משתמשים באבטחת רשת במחשבים אישיים וניידים, ו-55% משתמשים בה במכשירים ניידים - אבל רק 41% משתמשים באבטחת רשת במדפסות.[1]

כשמדובר באבטחת נקודות קצה, ההפרש גדול יותר:

בנוסף, פחות משליש (28%) מהמשיבים פורסים אישורי אבטחה למדפסות, בניגוד ל-79% שפורסים אישורים למחשבים אישיים ו-54% למחשבים ניידים.[1]

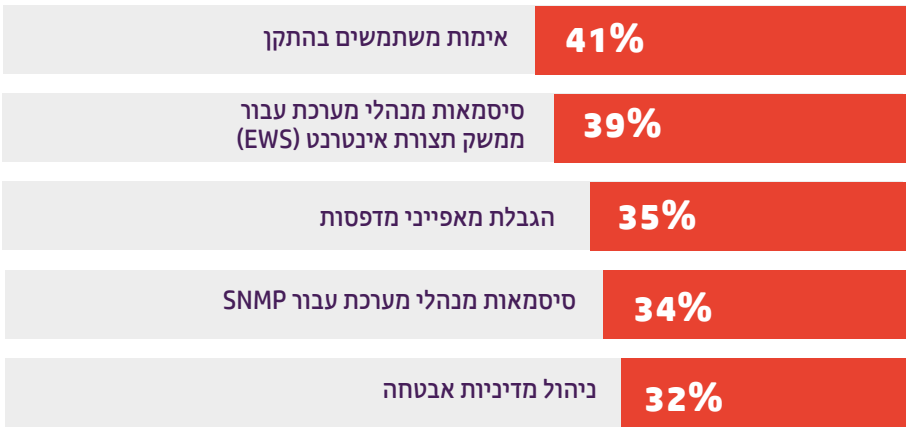
נוהלי אבטחה מובילים של נקודות קצה



בקרב ההגנות שמופעלות בהתקנים כלליים של נקודות קצה, אמצעי האבטחה הנפוצים ביותר עבור מדפסות היו אבטחת מסמכים, אבטחת רשת ובקרת גישה. עם זאת, פחות מחצי מהמשיבים אמרו שהארגון שלהם משתמש באחד מהאמצעים האלה במדפסות שלהם.[1]

בחלק מהחברות קיימים נהלים ספציפיים לאבטחת מדפסות, אבל גם הנהלים האלה שונים מאוד האחד מהשני. מעט יותר מ-40% מהארגונים פרסו אימות משתמשים, ופחות מ-40% השתמשו בסיסמאות מנהלי מערכת עבור ממשקי תצורת אינטרנט.[1] להשגת הגנה חזקה, כל ארגון צריך להשתמש בשילוב של הגישות האלה - ויותר מזה.

נוהלי אבטחה מובילים ספציפיים למדפסות



כשמדובר בנוהלי תאימות וביקורת של נקודות קצה, בקרות אבטחת המדפסות נותרות מאחור בהשוואה לכמעט כל נקודות הקצה האחרות. כמעט 90% מהארגונים פרסו מדיניות אבטחת מידע, אך המדיניות הזו בדרך כלל לא כוללת מדפסות. למשל, 57% מהמשתתפים פרסו הגנות מפני תוכנות זדוניות במחשבים האישיים שלהם, אך רק 17% פרסו הגנות כאלה במדפסות.[1]

כמעט 9 מתוך כל 10 מקצועני IT מספרים שהארגון שלהם מיישם מדיניות אבטחת מידע מהסיבות הבאות:

ברור שארגונים לא מתייחסים לאבטחת מדפסות ברצינות הראויה, אבל הם בהחלט צריכים לעשות את זה.

"חלק גדול מהמדפסות נשארו עם סיסמאות ברירת המחדל, או בלי סיסמאות בכלל, ובמקרים מסוימים אותה הסיסמה משמשת בעשר מדפסות", כך לדברי מייקל הוארד, יועץ אבטחה בכיר ב-HP, בראיון ל-Computerworld שנערך בחודש יוני. "מדפסת שאינה מוגנת באמצעות סיסמה היא מתנה אמיתית לפצחנים (האקרים). אחת מהפריצות הנפוצות שנתקלנו בה היא התקפת "אדם בתווך" (man-in-the-middle), שבה פצחנים משתלטים על מדפסות ומסיטים מסמכים נכנסים אל מחשב נייד לפני הדפסתם. הם יכולים לראות את כל מה שהמנכ"ל מדפיס."[2]

ההשלכות הפוטנציאליות של פריצות למדפסות

בוגדן בוטזאטו, אנליסט בכיר של אימים אלקטרוניים בחברת Bitdefender, מספר שמדפסות עשויות ליצור פרצת אבטחה משמעותית. "המעבדות שלנו להערכת נקודות תורפה מקבלות הרבה נתוני טלמטריה. הנתב הוא כבר לא ההתקן הכי הגרוע באינטרנט. הכבוד הזה עבר למדפסת."[3]

לנקודות התורפה האלה יכולות להיות השלכות נרחבות על העסק. מדפסת בודדה שאינה מאובטחת עלולה לחשוף רשת שלמה של התקנים מקושרים להתקפה, ולאפשר לפצחנים לרגל אחרי ההתקנים המרושתים שלך - וכך לפגוע באבטחה של הרשת כולה.

1. זמני תמיכה ארוכים יותר ושיחות ארוכות יותר במוקד התמיכה

2. פגיעה ביעילות/פרודוקטיביות

3. זמני השבתת מערכת ממושכים יותר

4. יותר זמן מושקע בשיחות לצורך תמיכה

5. אכיפה מוגברת של מדיניות משתמשי קצה

כולנו ראינו את ההשפעות של פרצות אבטחה. לדברי המשתתפים בסקר של Spiceworks, אלו חמש ההשפעות המובילות של פרצות:[1]

אבל פרצה במדפסת עלולה להיות חמורה אפילו יותר, ובמיוחד אם נעשה שימוש במדפסת רב-תכליתית המסוגלת לאחסן נתונים מודפסים באופן אלקטרוני.

עבודות הדפסה שמאוחסנות במטמון של המדפסת מאפשרות לפצחנים לגשת למידע עסקי או אישי רגיש.

יותר מזה, פצחנים יכולים לגשת לרשת הכוללת של החברה דרך מדפסת לא מאובטחת, ולגנוב פרטים כמו מספרי תעודות זהות, מידע פיננסי או תזכירים ומסמכים פנימיים. מעבר להשפעה של המידע הגנוב על העובדים, המידע הזה עשוי להגיע למתחרים או לגרום לפגיעה משמעותית במוניטין של החברה.

הפתרון הקל: מאפייני אבטחה מובנים

ברור שחברות צריכות לטפל בנושא האבטחה גם כשמדובר במדפסות. חלק מהמדפסות המודרניות ברמת הארגון כוללות מאפייני אבטחה מובנים ונוחים לשימוש, המגנים מפני איומים על מדפסות. המאפיינים האלה כוללים:

- זיהוי מתקפות, הגנה מפני מתקפות וטיפול בנזקים באופן אוטומטי
- מעקב אחרי השימוש כדי למנוע שימוש לא מאושר
- אפשרויות התחברות פשוטות כמו קודי PIN או כרטיסים חכמים
- קורא כרטיסים חכמים המאפשר למשתמשים לאמת את זהותם במהירות ולהדפיס בצורה מאובטחת מהמדפסת, תוך שימוש בתג הזיהוי שלהם.
- הדפסה מאובטחת ומוצפנת של מסמכים רגישים

לפני רכישת מדפסת חדשה, בין אם מדובר במדפסת שולחנית או במדפסת רב-תכליתית, מומלץ ללמוד על הגנות האבטחה המשולבות ולהפעיל אותן. עם מאפיינים פשוטים וספציפיים למדפסות כמו אלה, אין סיבה שמדפסות ימשיכו להוות נקודת תורפה. חשוב לזכור שבעידן ה-Internet of Things יש מספיק נקודות גישה אחרות שדורשות התייחסות - **המדפסות שלך לא צריכות להיות חלק מהן.**

מחפש מדפסות מאובטחות יותר?

מידע נוסף ›

מקורות:

1. סקר של Spiceworks, שכלל 309 מקבלי החלטות בצפון אמריקה, אזור EMEA ו-APAC. הסקר נערך מטעם HP בחודש נובמבר 2016.
2. "Printer Security: Is your company's data really safe?" *Computerworld*, 1 ביוני 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html
3. "Printers Now the Least-secure Things on the Internet", *The Register*, 8 בספטמבר 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/