אסטרטגיית היציאה של מרחב הסייבר

בחודשי הקורונה חלה עלייה חדה במספר הניסיונות של פושעי סייבר לנצל את השימוש הגבוה בשירותי ענן. בחברת מקאפי, המתמחה באבטחת מידע ארגוני ואישי, מדגישים כי נדרשת הגנה מלאה על הארגון ממכשיר הקצה ועד לענן | **שון הר-טוב**

אסטרטגיית היציאה ממשבר הקורונה רק יצאה לדרך, וכבר עתה ברור לכולנו ששגרת החיים ושגרת העבודה לא יהיו אלה שהכרנו עד לא מזמן.

אחד השינויים הבולטים שיצרה המציאות החדשה הוא התבססות המגמה של עבודה מרחוק, אשר התרחבה משמעותית עם פרוץ המגיפה וכוללת עתה גם מגזרים ועובדים שלא הורגלו בכך. חברות רבות אמנם התוודעו ליתרונות העבודה מרחוק, עבור הארגון כמו גם לעובדים, אולם הצורך לבצע את השינוי במפתיע ובזריזות, יצר לא מעט אתגרים וקשיים, שנבעו מהיעדר תכנון מקדים והבהירו שלעבודה מרחוק יש גם חסרונות.

"אחד האתגרים המשמעותיים עימם התמודדו ארגונים, שעובדיהם עברו לעבוד מהבתים, הוא ירידה משמעותית ביכולת להגן על תשתיות החברה הפיזיות כמו גם אלה שבענן", אומרת כוכבית אלמגור, מנהלת מקאפי ישראל וראש מרכז הפיתוח המקומי. "בחודשי הקורונה הוכפל השימוש של עובדים במכשירים בלתי מנוהלים - כגון לפטופ פרטי או מחשב ביתי שאינו מוגן על-ידי הארגון - דבר שהוסיף שכבת סיכון נוספת עבור אנשי האבטחה, שאחראים על הגנת הנתונים בענן. חלון הזדמנויות זה נוצל בזריזות ובהצלחה על-ידי פושעי סייבר ולכן ארגונים נדרשים כעת לתכנן בצורה אסטרטגית את המשך העבודה מרחוק".

צילום: אילון יחיאל

כוכבית אלמגור, מנהלת מקאפי ישראל: "כדי להגן על המידע באקלים הנוכחי, ארגונים צריכים לשלוט ולהכיר לעומק את סביבת המחשוב שלהם, את כל המשתמשים בה וכן את האיומים שאורבים לאורך מחזור החיים של המידע, בתוך הרשת הארגונית ומחוצה לה - וזו משימה לא פשוטה כלל"

דרושים מודלים מתקדמים של אבטחה

חברת אבטחת המידע מקאפי (McAfee) היא מובילה עולמית באבטחת מידע ארגוני ואישי ממכשירי הקצה ועד לענן. החברה מגינה על ארגונים עסקיים ועל עשרות מיליוני משתמשים ברחבי העולם, ומפעילה בישראל מרכז פיתוח אסטרטגי למוצרי החברה העתידיים, וכן פעילות עסקית מקיפה של מכירות ושירותים מקצועיים לכלל מגזרי המשק.

מדו"ח שפרסמה החברה החודש, עולה כי בין החודשים ינואר לאפריל השנה, חלה עלייה חדה במספר הניסיונות של פושעי סייבר לנצל את השימוש הגבוה בשירותי ענן, שזינק ב-50%, כדי לפרוץ ולפגוע בארגונים. מספר האיומים החיצוניים זינק בחודשי הקורונה והגיע לפי-שבעה מתחילת השנה, כאשר מרבית ההתקפות היו ניסיונות להיכנס לחשבונות ענן בעזרת סיסמאות גנובות בהיקפים גדולים. הם התמקדו בעיקר בשירותי ענן לעבודה משותפת כמו Microsoft 365.

לדברי אלמגור, "מגמות אלה מדגישות את הצורך במודלים מתקדמים של אבטחה. חשוב שארגונים ישמרו על רציפות עסקית גם בתקופה של ריחוק חברתי, אך עליהם לעשות זאת באופן מאובטח כדי למנוע אפשרות של אובדן נתונים כתוצאה ממתקפת סייבר. כדי להגן על המידע באקלים הנוכחי, ארגונים צריכים לשלוט ולהכיר לעומק את סביבת המחשוב שלהם, את כל המשתמשים בה וכן את האיומים שאורבים לאורך מחזור החיים של המידע, בתוך הרשת הארגונית ומחוצה לה - וזו משימה לא פשוטה כלל".

הגנה רציפה על כל נכסי המידע

לפי נתונים של מקאפי, אתגרי אבטחת המידע נמצאים במגמת עלייה גם ללא קשר לקורונה עקב העלייה העקבית בשימוש העולמי בשירותי ענן. כך למשל, בין השנים 2016-2019 מספר הקבצים שהכילו מידע עסקי רגיש בענן גדל מדי שנה ב-23%. אולם עדיין, מעל למחצית הארגונים (52%) משתמשים בשירותי ענן שכבר נפלו בעבר קורבן לפריצה ולגניבת נתוני משתמשים, ורק ל-31% מהארגונים יש פתרון להגנת המידע באופן רציף ממכשירי הקצה, דרך הרשתות ועד לשירותי הענן שלהם.

צילום: MAMA-Mati & Mark

יניב נזרי, מנהל הפעילות העסקית של מקאפי בישראל: "חשוב לדאוג להגנה רציפה על כל נכסי המידע בסביבת העבודה המבוזרת, אשר כוללת מכשירי קצה מגוונים (מנוהלים ובלתי-מנוהלים), רשתות ארגוניות, וכן שירותי ענן שונים"

"שירותי ענן מספקים לארגונים מגוון עצום של יתרונות והזדמנויות, אך גם סיכונים חדשים שצריך להכיר ולהיערך לקראתם", טוען יניב נזרי, מנהל הפעילות העסקית של מקאפי בישראל, "ולכן חשוב לדאוג להגנה רציפה על כל נכסי המידע בסביבת העבודה המבוזרת, אשר כוללת מכשירי קצה מגוונים (מנוהלים ובלתי-מנוהלים), רשתות ארגוניות, וכן שירותי ענן שונים.

"המעבר לשימוש בשירותי הענן הוא בלתי נמנע, ולכן אנו ממליצים לארגונים לנקוט בחשיבה ובגישה של cloud-first בכל הנוגע לאבטחת המידע שלהם. גישה זו כוללת כלים ומערכות אבטחה, שפותחו עבור העולם החדש ומתאימים במיוחד לענן", מוסיף נזרי. "חלק לא מבוטל מלקוחותינו משתמשים כיום במודל ענן היברידי, ואנו ערוכים היטב כדי לספק להם את רמת האבטחה הגבוהה ביותר גם בסביבות אלה, תוך שאנו תומכים במעבר ההדרגתי שלהם לענן".

למקאפי יש יכולות מתקדמות ביותר לזיהוי ועצירת מתקפות סייבר בעידן הענן. האסטרטגיה של החברה מתבססת על מערכת אינטגרטיבית ופתוחה, המספקת הגנה מלאה על המידע הארגוני ממכשירי הקצה ועד לענן, כדי למנוע דליפות ואובדן מידע, ולעצור אירועי סייבר התקפי.

אבטחה פרואקטיבית

"אנו ממוקדים מאוד בבנייה ואופטימיזציה של סביבות אבטחה מבצעיות עבור לקוחותינו על בסיס MVISION, הפורטפוליו העשיר שפיתחנו בגישת cloud-first", מספרת אלמגור. מדובר, לדבריה, באסטרטגיה שלמה שיושמה במערך חדשני של פתרונות מבוססי ענן לעציר איומים ולאבטחת המידע בכל מחזור החיים שלו - ממכשירי הקצה, דרך הרשת הארגונית ועד לשירותי ענן (Iaas, Paas, SaaS) וכמובן סביבות on-prem.

"הערך הרב ש-MVISION מספק ללקוחותינו מתבטא בכמה היבטים: יותר גמישות ותמיכה בטרנספורמציה לענן, יותר יכולת הכלה עם אפשרות לנהל ארכיטקטורה של פלטפורמה פתוחה, והגנה רחבה יותר בכל פלטפורמה וסביבת מחשוב שהיא".

נזרי מוסיף, כי "מקאפי משתמשת במחזוריות של הגנה רציפה (Protect-Detect-Correct) כעקרון בסיסי בפיתוח כל מוצרי האבטחה שלה. טכנולוגיות וכלי אבטחה מבודדים אינם מסוגלים לשתף מידע בצורה אוטומטית לטובת מודיעין אבטחה. אך בסביבות אבטחה פרואקטיביות, ברגע שאיום כלשהו מזוהה, אז כל המערכות (כולל מערכות צד שלישי) מעודכנות ומוגנות מפניו באופן מיידי.

"כדי להפחית את רמת המורכבות של מערך האבטחה הארגוני", הוא מוסיף, "מומלץ לאחד כמה שיותר בין פתרונות הגנה בענן וברשת האינטרנט, על מנת להגיע לשליטה מלאה בשירותי ענן שהעובדים משתמשים בהם - בין אם מאושרים ובין אם לא".

הענן מהווה כר פורה להאצת חדשנות ולהנגשת שירותים מתקדמים. הוא מגלם בתוכו עולם שלם של הזדמנויות חדשות, עסקיות וטכנולוגיות, ויכול לסייע רבות לארגונים בתקופת הקורונה ואף לאחריה. צריך רק לזכור, כפי שמציינים בכירי מקאפי בישראל, שעל מנת להפיק מהענן את מלוא הפוטנציאל מבלי להיפגע, יש להיערך להגנה מתאימה על כל נכסי המידע הארגוני - החל ממכשיר הקצה ועד לקצה הענן.