Microsoft Security

CSO

מודל אבטחה של 'אפס אמון':
שיעורים מהלקוחות שהקדימו לאמץ את הפתרונות שלנו

Microsoft Security

CSO

תוכן העניינים

- מבוא
- 'אפס אמון' כבר כאן, ומספק ערך
- גורמים מניעים לפריסה לפי גישת 'אפס אמון'
- אין מחסור באיומים
- מכשולים העומדים בפני אימוץ מודל של 'אפס אמון'
- אתגרי פריסה
- שיטות עבודה מומלצות להטמעת מודל 'אפס אמון'
- היכן אתה ממוקם במסלול אל מודל 'אפס אמון'?

Microsoft Security CSO

מבוא

השנתיים האחרונות, הרוויות בשיבושים, ערערו את המודלים המסורתיים של IT ואבטחה. כתוצאה מכך, אבטחת 'אפס אמון' התפתחה במהירות והפכה מרעיון מעניין לבסיס לאבטחה ארגונית מודרנית.

מחקר חדש של Foundry מראה כי 52% מהארגונים בוחנים או שכבר פרסו ארכיטקטורת 'אפס אמון', ו- 15% נוספים חוקרים מודלים של 'אפס אמון'. מאמצים אלה מדווחים על יתרונות רבים הודות לפריסות שלהם, כולל הגנה משופרת על נתוני לקוחות, הפחתת המורכבות ומתן גישה אמינה ומאובטחת למשאבי הארגון.

ספר אלקטרוני זה יסקור את תוצאות המחקר של Foundry, המדגיש את חשיבות אסטרטגיית 'אפס אמון' לצורך סיוע לסמנכ"לי אבטחת מידע (CISOs) להגן על הארגונים שלהם מפני מגוון סיכונים מגורמי תקיפה שונים. הוא כולל גם הדרכה לגבי הטמעת 'אפס אמון' עבור אלה המתחילים את מסעם.

אודות הסקר

Foundry ביצעה סקר עסקים בארה"ב בפברואר ומרץ 2022 כדי לסקור את המצב הנוכחי של אימוץ מודל 'אפס אמון'. המשיבים לסקר נדרשו להיות מנהלי IT או בכירים יותר בחברה המעסיקה יותר מ- 500 עובדים, שתפקידם קושר אותם לרכישת מוצרים ושירותים של אבטחת סייבר.

היו בסך הכול 250 משיבים בסקר בן 23 שאלות.

Microsoft Security

CSO

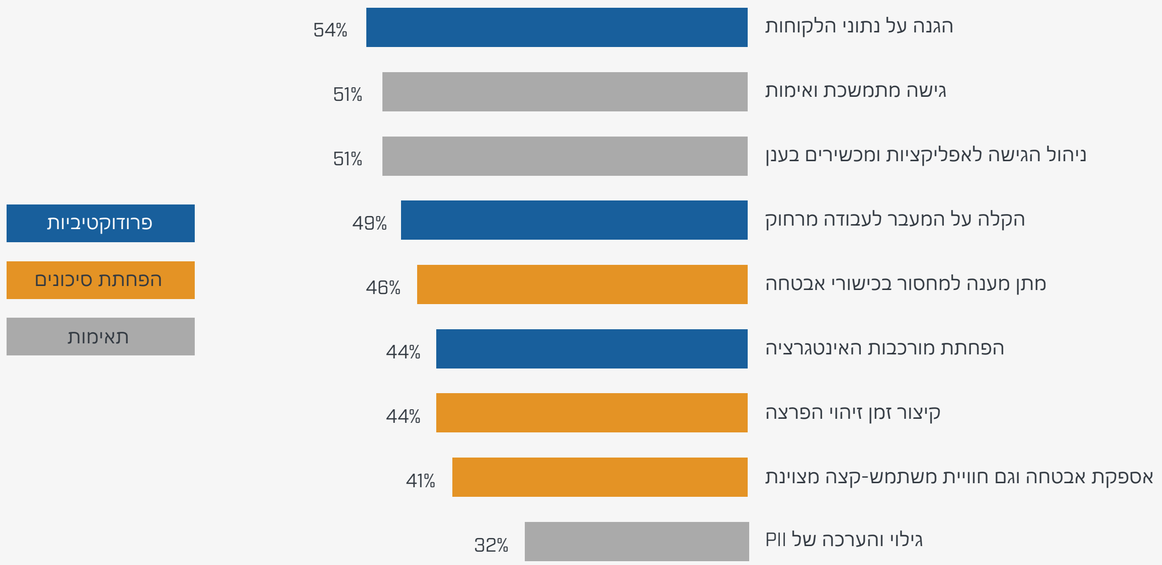
'אפס אמון' כבר כאן, ומספק ערך

מתוך תוצאות הסקר מתברר, בנוסף לראיונות עומק שנערכו עם מומחי IT ואבטחה, כי 'אפס אמון' נמצא בראש סדר העדיפויות. ואלו שפרסו רכיבים שונים של 'אפס אמון' כבר נהנים מהיתרונות.

רוב המשיבים שהטמיעו את 'אפס אמון' (87%) אומרים שהארכיטקטורה מספקת תוצאות התואמות או אף עולות על היעדים המקוריים שלהם להטמעה, אימוץ ואינטגרציה.

"['אפס אמון'] הפך להליך תפעול סטנדרטי אצלנו. אני לא חושב שנוכל אי פעם לחזור למה שהיינו קודם," אומר מנהל IT בחברה קמעונאית גלובלית. (למשיבים הובטח שפרטיהם יישארו חסויים בתמורה לכך שידברו באופן חופשי על תוכניות האבטחה שלהם.)

יתרונות בעקבות הטמעת מודל 'אפס אמון'



12% מהמשיבים אמרו שהם משיגים את *כל* היתרונות האלו

מקור: סקר של Foundry בנושא אימוץ מודל 'אפס אמון', מרץ 2022 בסיס: 250

Microsoft Security

CSO

כ- 44% מהמשיבים גם דיווחו ש'אפס אמון' צמצם את המורכבות הטבועה בהטמעת ארכיטקטורת אבטחה משולבת. "מכיוון שמדובר במסגרת שאתה עובדים, זה הופך דברים לפחות מסובכים," אומר סמנכ"ל האבטחה של חברת מוקד שירות שמעסיקה 3,500 עובדים.

סמנכ"ל אבטחת מידע בחברה לשירותים פיננסיים המעסיקה 17,000 עובדים אומר שהם מרוצים מאוד מהאימות הרב-גורמי שהחברה הטמיעה כחלק מ'אפס אמון'. "שביעות הרצון בקרב העובדים עלתה, כי עכשיו הם כבר לא צריכים להשתמש רק במחשבי החברה ובלקוח VPN, אלא יכולים להתחבר למשאבים מכל מקום," הוא אומר.

הרעיון של הרשאת גישה מינימלית השתלם גם הוא, מציין הסמנכ"ל. "מנהלי מערכת ביצעו פחות טעויות קטסטרופליות בזכות הטמעת מערכת הרשאת גישה מינימלית," הוא אומר. "הם מקבלים הרשאות עבור דברים מסוימים במסגרות זמן מסוימות, וזה מצמצם את הסיכוי לטעויות."

בשל השכיחות הגבוהה של הונאות דיוג ותקיפות סייבר אחרות, מנהל IT בחברה קמעונאית מסכם את היתרונות של 'אפס אמון': "אם לא היו לנו הכלים הללו, היינו כנראה במצב רע, כשאנו נאלצים לשלם למישהו בביטקוין כרגע."

Microsoft Security CSO

גורמים מניעים לפריסה לפי גישת 'אפס אמון'

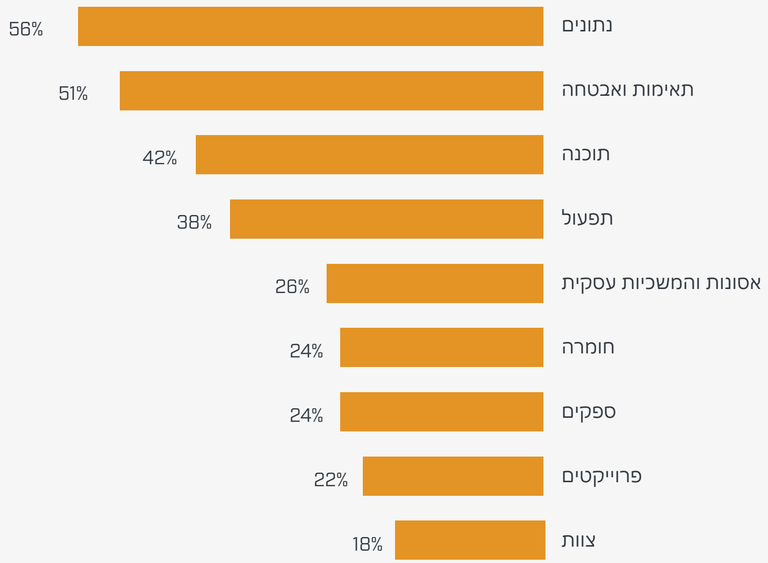
מפגש בין אירועים דוחף חברות לשקול לכל הפחות ארכיטקטורה של 'אפס אמון'. בראש הרשימה נמצא הצורך לנהל סיכונים עבור מגוון משאבים כנגד ריבוי איומים. המשיבים לסקר ייחסו תקריות אבטחה ששקולות לשנה למספר סיבות, ובראשן פגיעויות אבטחה מצד שלישי, מיחידים או מארגונים. סיבות אחרות כללו:

- סיכונים עסקיים לא צפויים
- הגדרת תצורה שגויה של שירותים או מערכות
- תקיפות זדוניות מכוונות מצד גורם פנימי
- שגיאות משתמש ללא כוונת זדון, כולל קורבנות דיוג
- חשיפת זהויות
- תוכנה ללא תיקונים
- אישורים שנגנבו

תקריות אלה מהוות מספר סיכונים, ובראשם נתונים.

עבור ארגונים רבים, המעבר הפתאומי לעבודה מרחוק שנגרם על-ידי המגפה, האיץ תוכניות אימוץ של מודל 'אפס אמון', כשמודלים מסורתיים של אבטחה, המבוססים על היקפים, הפכו למיושנים. ארגונים רבים כבר היו בכיוון, כשהעבירו יותר יישומים ותשתיות IT לענן, אך המגפה נתנה דחיפה נוספת.

קטגוריות מובילות בסיכון מאיומי אבטחת סייבר



מקור: סקר של Foundry בנושא אימוץ מודל 'אפס אמון', מרץ 2022 בסיס: 250

Microsoft Security CSO

לדוגמה, סמנכ"ל אבטחת מידע בחברת טכנולוגיה רפואית בת 1,700 עובדים אומר שהענן והמגפה הובילו אותו לאמץ את מודל 'אפס אמון', שכעת מהווה בסיס בטוח לכל מודל עתידי של מקומות עבודה.

"המניעים העסקיים היו עצם העובדה שאנחנו חברה מבוססת ענן וזקוקים ליכולת להגן על הסביבה שלנו," הוא אומר. "היינו גם צריכים לספק כוח עבודה שיהיה מסוגל לעבוד מרחוק במהלך המגפה. ['אפס אמון' אפשר לנו לצמצם באופן דרמטי את טביעת הרגל הנדל"נית שלנו, וכנראה שנישאר חברה שהיא לפחות 60% וירטואלית ומרחוק."

Microsoft Security CSO

אין מחסור באיומים

צורכי תאימות סיפקו גם הם תנופה לעבר מודלים עמידים יותר של אבטחה. "רגולטורים צופים בנו, ומצפים מאתנו להמשיך ולשפר את מסגרת האבטחה שלנו," אומר סמנכ"ל אבטחת מידע גלובלי בחברת שירותים פיננסיים עם 290,000 עובדים.

ארגונים מסוימים יזמו צעדים לעבר 'אפס אמון' כדי למנוע פרצה בפרופיל גבוה שתציב אותם באור הזרקורים מהסיבות הלא-נכונות. "רצינו להיות פרואקטיביים וניסינו להישאר מחוץ לחדשות," מספר סמנכ"ל טכנולוגיות מידע במוסד להשכלה גבוהה עם 3,500 עובדים. "ישנם סיפורי זוועות של ממש על מוסדות מקומיים אחרים בגודל דומה שהושבתו לזמן רב."

אחרים כבר חוו תקרית רצינית של אבטחת סייבר, שאילצה אותם לבחון מחדש את אסטרטגיית האבטחה שלהם. לאחר שחברת ביטוח עם 6,000 עובדים סבלה ממתקפת כופרה שהשביתה את הרשת הארגונית למשך שבועיים, הדרישה לאמץ את מודל 'אפס אמון' הגיעה ישירות מהמנכ"ל. "האצנו מאוד את ההטמעה," אומר סמנכ"ל פיתוח ה- IT בחברה. "בהתחלה, זה היה ברמה של שיטות עבודה מומלצות, ואז זה האיץ מאוד לאחר מתקפת הכופרה שחווינו."

זרז המבוסס על ענן

סמנכ"ל אבטחת המידע בחברה גדולה לשירותים פיננסיים מספר שהצוות שלו זיהה את הצורך בארכיטקטורת אבטחה חדשה כבר לפני מספר שנים, כשהחל לאמץ יותר משאבים מבוססי ענן והמשתמשים הפכו לניידים יותר.

"הבנו שארכיטקטורת המבצר המסורתית שלנו, שעליה הסתמכנו בעבר, לא הייתה ערוכה להגן עלינו מפני תקיפות בעתיד," הוא אומר.

מציאות זו הפכה לברורה מאוד בשנת 2020, כאשר התגלה שבמהלך השנה הקודמת חדר תוקף אל היקף החברה ונע באופן רוחבי בתוך הסביבה בלי להתגלות. "הזדקקנו לארכיטקטורה שבה נוכל להגן ולאמת את השימוש במשאבים אלה, במקום בו הם נמצאים, וארכיטקטורת 'אפס אמון' בנויה לכך."

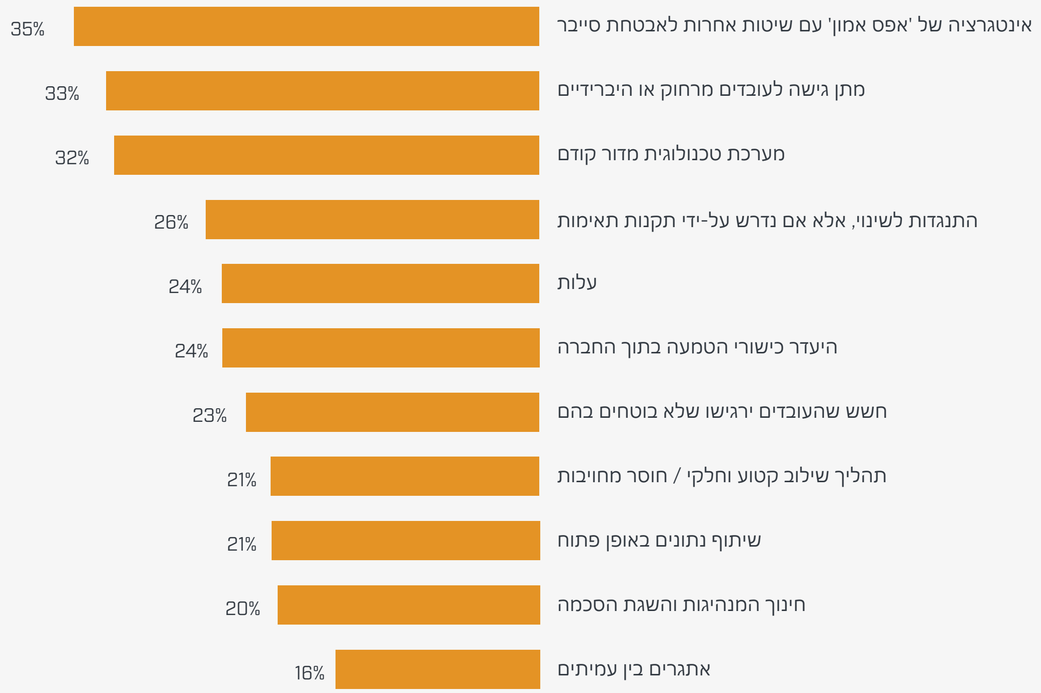
Microsoft Security CSO

מכשולים העומדים בפני אימוץ מודל של 'אפס אמון'

מודל 'אפס אמון' מייצג עבור ארגונים רבים שינוי יסודי במבנה, תהליך והלך רוח של אבטחה - מה שמסביר כמה מהמכשולים שעליהם יש להתגבר לפני אימוצו.

”היו כל כך הרבה מאגרי נתונים נפרדים שבהם נתקלנו בתוך הארגון," ציין סמנכ"ל אבטחת המידע במוקד, כשהסביר שלכל אחד מצוותי השרת, הרשת ובסיס הנתונים היה מערך עצמאי של שרתי אינטרנט וכלים. "זה האט אותנו כי לכל אחד היה רעיון שונה לגבי הכיוון והביצוע של העבודה."

מה מונע אימוץ של מודל 'אפס אמון'?



מקור: סקר של Foundry בנושא אימוץ מודל 'אפס אמון', מרץ 2022. בסיס: 250

Microsoft Security

CSO

חשיפת בעיות כאלה עשויה להיות תופעת לוואי חיובית של 'אפס אמון', לפי דבריו של אנתוני מוקני, מנהל שיווק מוצר בכיר של 'אפס אמון' ב- Microsoft. "כארכיטקטורה, 'אפס אמון' נועד לשבור את ההפרדה בין צוותי אבטחה שנמצאים בין עמודי תווך טכנולוגיים ולעזור לצוותים לעבוד ביחד בצורה מלוכדת," הוא אומר. "ייתכן שמדובר גם בשינוי תרבותי, בדרך שבה צוותים עובדים יחד."

עבור סמנכ"ל אבטחת האיכות בחברת השירותים הפיננסיים, אפליקציות מדור קודם היוו מכשול שעליו יש להתגבר בדרך אל 'אפס אמון'. "הן צריכות לעבור התאמה לטכנולוגיית אימות מודרנית," הוא אומר. "כתלות בגיל האפליקציות, זה לא דבר קל לביצוע."

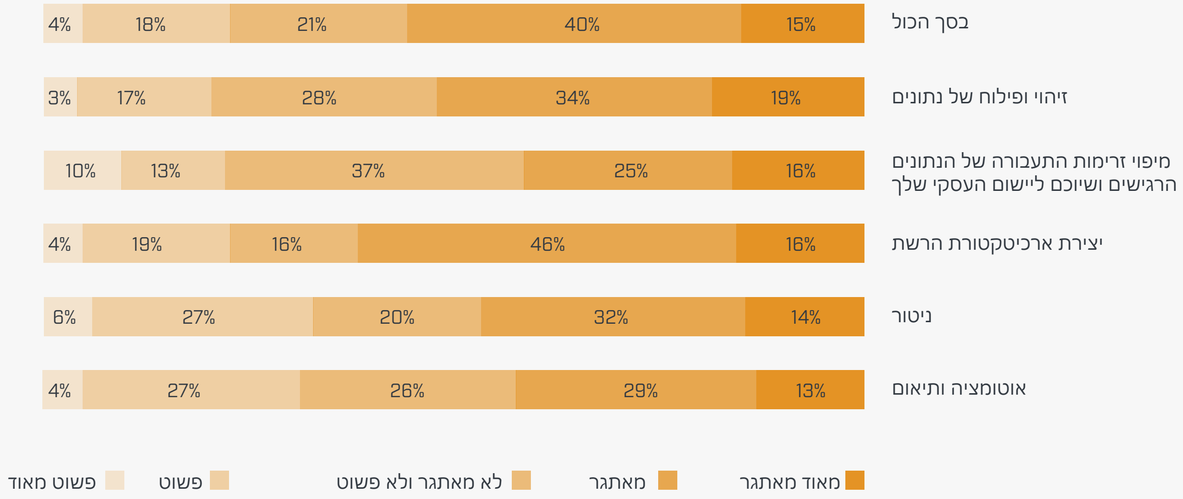
Microsoft Security

CSO

אתגרי פריסה

ברגע שחברות יוצאות למסע 'אפס אמון', עלולים לצוץ גם מגוון אתגרי הטמעה. יותר ממחצית המשיבים על הסקר (56%) הכירו בכך שהטמעת 'אפס אמון' הייתה מאתגרת או מאתגרת מאוד. באופן ספציפי:

עד כמה מאתגרת הטמעת 'אפס אמון'?



מקור: סקר של Foundry בנושא אימוץ מודל 'אפס אמון', מרץ 2022. בסיס: 168

אתגרים סביב פילוח ומיקרו-פילוח עלו לעתים קרובות בראיונות העומק.

"מבצעים פילוח של הרשת עד לרמת המארח הבודד," אומר סמנכ"ל אבטחת המידע בחברת השירותים הפיננסיים. "הדבר דומה להקמת 'חומת אש' קטנה בין כל מארח ומארח ברשת הפנימית, כך שאפשר לראות את התעבורה כולה ולשלוט בה עד לרמת המחשב הבודד. יש לכך יתרונות אבטחה עצומים, אבל זה קשה מאוד ליישום כי עכשיו צריך בעצם לנהל עשרות אלפי חומות אש."

גם תהליך מיפוי זרימות תעבורה עשוי לארוך חודשים. סמנכ"ל טכנולוגיות בחברת פרסום ומדיה המעסיקה 5,000 עובדים מספר כי לאחר הגדרת המידע הקריטי, האפליקציות ושירותי הרשת שעליהם צריך להגן, "מיפינו זרימות של טרנזקציות ברשת וניסינו להבין אותם כקבוצות מידע". "[ואז] ביצענו פילוח של חלקי המידע האלו וכיצד הם נעים לרוחב הרשת, עד לרמת מנות רשת בודדות." בנקודה זו, החברה הטמיעה מדיניות 'אפס אמון' לכל סוג של זרימת תעבורה. "הכנסנו גם יכולות חדשות לניטור ותחזוקה של הרשת שלנו."

למרות האתגרים, משיבים רבים מאמינים כי 'אפס אמון' למעשה מפשט את התפעול היומיומי. בטכנולוגיות מסורתיות, "ביצוע שינויים נמשך ימים; צריך להפיץ אותם ברחבי כל רכיבי החומרה והתוכנה, ואנחנו משתמשים בהמון משאבים לצורך כך," מספר סמנכ"ל אבטחת המידע בחברת השירותים הפיננסיים. "כשמדובר ב'אפס אמון', יש צמצום משמעותי במורכבות הארכיטקטורה בטווח הארוך ובמספר העובדים הנדרשים לביצוע אותו סוג עבודה."

שיטות עבודה מומלצות להטמעת מודל 'אפס אמון'

ככל שיותר חברות מטמיעות ארכיטקטורה של 'אפס אמון', הן מפתחות מפות דרכים ושיטות עבודה מומלצות שאחרים יכולים לפעול לפיהן. הנה חמישה שיקולים בעת תכנון פריסה.

לא ליצור עומס כבר בהתחלה

מיפוי אסטרטגיית 'אפס אמון' עלול להרתיע אם מסתכלים עליו רק בהקשר הרחב של שינוי מדיניות והגנות ברחבי רשתות, נתונים אפליקציות, זהויות, נקודות קצה ותשתית. "בהתחלה, הסתכלנו על ההר העצום שעליו יש לטפס ושאלנו את עצמנו אם באמת נעשה זאת," מספר סמנכ"ל טכנולוגיות מידע במוסד להשכלה גבוהה. "צריך להתקדם צעד אחד בכל פעם."

סמנכ"ל טכנולוגיות המידע והצוות שלו אימצו את הגישה "לך בעקבות הכסף", והציבו בראש סדר העדיפויות את פילוח האפליקציות הפיננסיות והשכר על רשת נפרדת.

לפי מוקני, זיהוי הנכסים הקריטיים ביותר שעליהם יש להגן זו גישה נכונה. "צריך להיות מודעים לסיבת היישום של 'אפס אמון' מלכתחילה," הוא אומר.

אם יש ספק, יש להתחיל עם אימות רב-גורמי

בעת קביעת סדרי העדיפויות של מערך האבטחה, סמנכ"לי אבטחת מידע וספקי אבטחה רבים ממליצים להתמקד תחילה באימות ובהגנות אחרות המבוססות על זהות. "אם אין לכם נקודת מוצא, אימות רב-גורמי הוא רעיון טוב," אומר מוקני.

ב- Microsoft מעריכים שאימות רב-גורמי יכול למנוע יותר מ- 90% מהתקיפות מבוססות הזהות.

סמנכ"ל אבטחת המידע בחברת השירותים הפיננסיים מסכים. "אימות הוא רכיב יסוד ביישום ארכיטקטורה של 'אפס אמון'. אף אחד מהרכיבים האחרים לא יעבוד ללא אימות זהותו של משתמש הקצה, אז התחלנו משם."

לאחר מכן, סמנכ"ל מערכות המידע טיפל ברכיב העבודה ברשת, והתוצאה הייתה יתרונות מידיים לתמיכה בעובדים מרחוק. הצוות השאיר את נושא המיקרו-פילוח לשלב מאוחר יותר במסע, כיוון שאין לו ניראות מידית לעסק בכללותו. "לאחר הביצוע, רמת האבטחה עולה באופן משמעותי, אבל אף אחד לא מרגיש בהבדל," הוא אומר.

Microsoft Security CSO

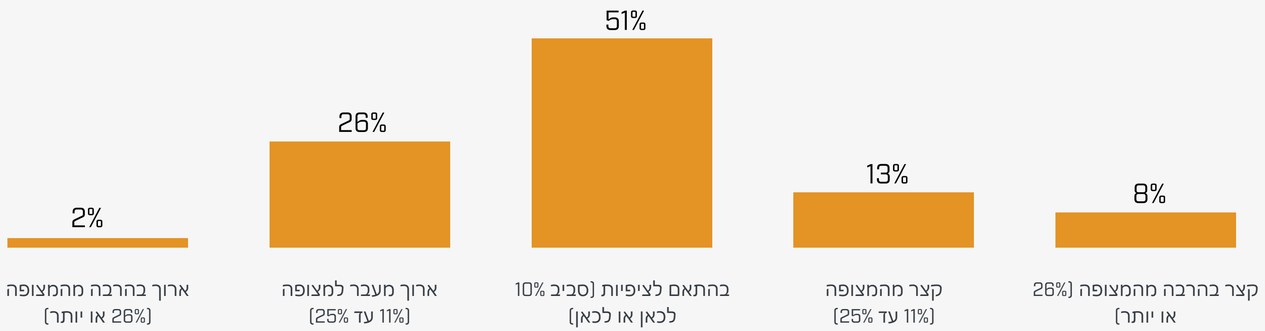
להיות מציאותי לגבי צירי הזמן

חשוב שסמנכ"לי אבטחת מידע יגדירו ציפיות מציאותיות לגבי פריסות 'אפס אמון'. "יישום ארכיטקטורת 'אפס אמון' הוא תוכנית ולא פרוייקט," אומר סמנכ"ל אבטחת המידע בחברת השירותים הפיננסיים. "זה היה שינוי עצום. ביצוע נכון כולל פרוייקטים רבים, וזה כנראה לאורך שנים; לא קיים יישום מהיר וקל של ארכיטקטורת 'אפס אמון'."

עמיתו, סמנכ"ל אבטחת המידע, מסכים. "אני לא חושב שנסיים אי פעם כי תמיד יש טכנולוגיות חדשות, תוכנות זדוניות חדשות, איומים חדשים," הוא אומר.

רוב המשיבים על הסקר (72%) אומרים שצירי הזמן שלהם לפריסה היו מדויקים או שהתקדמו מעל למצופה, והשאר אמרו שמשך היישום התארך מעבר למצופה.

"האם 'אפס אמון' עומד ביעדי ציר הזמן שלך?



מקור: סקר של Foundry בנושא אימוץ מודל 'אפס אמון', מרץ 2022. בסיס: 168

Microsoft Security

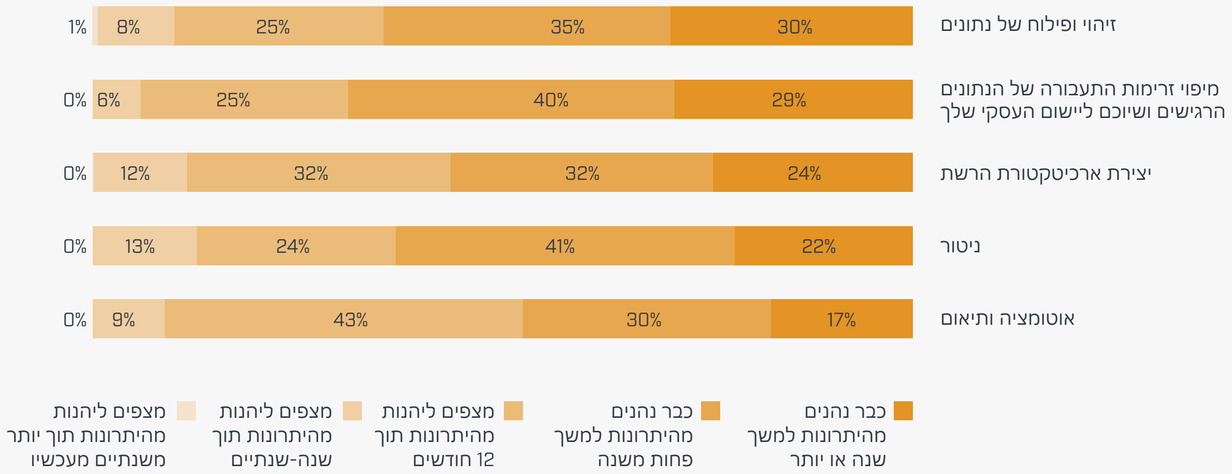
CSO

למדוד בהתאם לביצוע

בזמן שפריסת 'אפס אמון' מתרחשת, סמנכ"לי אבטחת מידע יכולים וצריכים ליצור אבני דרך למדידת ההתקדמות. כשני שליש מהמשיבים לסקר אמרו שהם נהנו מיתרונות מתוך רוב היבטי הפרוייקטים שלהם תוך שנה, וזה סימן טוב. רבע נוסף או יותר מצפים ליהנות מכך תוך 12 חודשים, ברחבי פעילויות עיקריות כגון זיהוי ופילוח של נתונים, מיפוי זרימות תעבורה ותכנון ארכיטקטורת הרשת.

"'אפס אמון' זה מסע, בשל ההערכה המתמדת שצריך לבצע כדי להגן מפני תקיפות שאופיין משתנה תמיד," אומר מוקני. "תמיד צריך לחפש שיפורים."

ציר זמן כדי ליתרונות 'אפס אמון'



מקור: סקר של Foundry בנושא אימוץ מודל 'אפס אמון', מרץ 2022. בסיס: 103

Microsoft Security CSO

להתמקד באנשים, לא רק בטכנולוגיה

למודל האבטחה של 'אפס אמון' יש טווח הגעה רחב והוא משפיע על כל העובדים, כולל צוותי ה- IT והאבטחה שעליהם הוטל לפרוס אותו. זו הסיבה שבגללה חשוב לוודא, כמו בכל פרוייקט טכנולוגי גדול, שהפריסות מסונכרנות עם תהליכים חדשים ולשנות את שיטות הניהול כדי להבטיח פריסה חלקה ומוצלחת.

"בנוסף לשינוי הטכנולוגי, ישנו גם שינוי תרבותי," אומר מוקני. "אם ישנם מספר צוותים שמטפלים באבטחה – כולל מהנדסי רשת או מומחי זהות – צריך גם לשנות את האופן שבו צוותים אלה עובדים ביחד. צריך לפרק מאגרי נתונים נפרדים כדי לוודא שהטכנולוגיה עובדת כולה כמקשה אחת."

פירוק מאגרי נתונים נפרדים מצריך כינוס צוותים מכל התחומים הללו לצורך ביצוע פרוייקטים של פיילוט והוכחת היתכנות (POC). מנהל מערכות מידע בחברת טלקומוניקציה המעסיקה כ- 2,000 עובדים למד את הלקח לאחר שהתמודד עם מספר נקודות כשל בודדות במהלך הפריסה, כולל שירותים שלא ניתן היה לאמת ונחשבו פתאום ל"לא מהימנים", דבר שהוציא אותם ומערכות מסוימות משימוש.

"פריסת שירות אחד עלולה להשפיע על כל השאר, כמו בדומינו, ולהפיל אותם," הוא אומר. בהמשך הדרך, "אנחנו זהירים הרבה יותר – יותר זמן מוקדש להוכחת היתכנות (POC), סקירות, ובדיקות ארכיטקטורה עם מומחים בנושא לפני הפריסה."

החזר השקעה (ROI) של 'אפס אמון'

מחקר שהוזמן על ידי Microsoft בשנת 2021 **The Total Economic Impact™ ובוצע על ידי Forrester Consulting** מכמת את החיסכון בעלויות והיתרונות העסקיים של פתרונות 'אפס אמון' מבית Microsoft. בהתבסס על חמשת הארגונים שהשתתפו בראיון של חברת Forrester, ארגון מורכב נהנה מהחזר השקעה (ROI) של 92% במהלך שלוש שנים כתוצאה מהטמעת ארכיטקטורת 'אפס אמון' של Microsoft.

ארגון מורכב זה גם חסך 20 דולרים בממוצע לעובד לחודש על ידי ביטול הצורך בכלי אבטחה שהפכו למיותרים לאחר הטמעת מודל 'אפס אמון', כולל ניהול נקודות קצה, תוכנות אנטי-וירוס, ופתרונות כנגד תוכנות זדוניות.

Microsoft Security CSO

היכן אתה ממוקם במסלול אל מודל 'אפס אמון'?

הסקר מראה כי יתרונות מודל האבטחה של 'אפס אמון' עולים בבירור על כמה מאתגרי הפריסה שעמם מתמודדים סמנכ"לי אבטחת מידע וצוותי האבטחה שלהם. התמודדות עם אתגרים אלה בעזרת תוכנית מתוכננת היטב עשויה לעזור לארגון שלך לשפר את ההגנות במהירות, להפחית סיכונים, ולהתחיל לספק ערך ברחבי העסק.

כדי להעריך את רמת בשלות 'אפס אמון' של הארגון שלך ולקבל משאבים מעשיים נוספים לפריסה, יש לבצע את **הערכת הבשלות לקראת מודל 'אפס אמון' של Microsoft**.