05

ביקורת סייבר מונחית מדדים

גיל גזית

מר גיל גזית הוא מנהל ביקורת באגף לביקורת אבטחת המידע והגנת הסייבר בחטיבה לביקורת משרדי הממשלה ומוסדות השלטון שבמשרד מבקר המדינה ונציב תלונות הציבור.

המאמר בקצרה

- מאמר זה מציג גישה בביקורת סייבר המיועדת להפיק ממצאים מדויקים ואובייקטיביים ככל האפשר על מצבם של גופים מבוקרים בהיבטי הגנה בסייבר - ביקורת מונחית מדדים.
- גישה זו נועדה בין השאר לשפר את יכולת איתור הפערים המרכזיים ולתמוך בצורה משופרת בתהליכי קבלת החלטות בגופים בנוגע לתיעדוף הטיפול בפערים ולתקצובו.
- המאמר מתבסס בין השאר על תקן NIST SP 800-55v1.
- המאמר מגדיר את נושא המדידות בביקורת סייבר, מציג ברמת-על תהליך של הגדרת מדדים, נותן דוגמאות קונקרטיות ומספק הצצה לעתיד התחום.

מבוא | מדידות בביקורת סייבר | ערכי סף ועידן ה- AI | סיכום

מבוא

בשנים האחרונות, מתוך הבנת המשמעות האסטרטגית של הנושא, שם מבקר המדינה מר מתניהו אנגלמן דגש על ביקורות בתחום ההגנה בסייבר. ביקורות מתבצעות הן כביקורות ייעודיות ואם העניין מתבקש - כפרקים בתוך ביקורות בנושאים אחרים.

יעד מרכזי של ביקורת המדינה הוא טיוב פעולת הגופים המבוקרים וקידום של מילוי ייעודם ושל התועלת לציבור[1]. לשם כך ביקורת המדינה פועלת לאיתור ליקויים ופערים ולמציאת בעיות השורש והחסמים המרכזיים.

היבטי הסייבר בייעודם ובפעולתם של הגופים המבוקרים

הגופים המבוקרים פועלים וממלאים את ייעודם גם **במרחב הדיגיטלי**, היבטי מינהלה, היבטי שירות לציבור, בהיבטים אופרטיביים (כגון OT) ובהיבטים נוספים.

אסטרטגיית הסייבר הלאומית שפרסם מערך הסייבר הלאומי בפברואר 2025 מגדירה את **החזון הלאומי** בתחום זה כ"מרחב דיגיטלי **אמין**, **זמין ובטוח** המאפשר את היתרונות של עולם משגשג ומתקדם". המסמך מגדיר את שלושת המרכיבים העיקריים הכלולים בו:

אמינות - היכולת לסמוך על אותנטיות המידע, על התוכן ועל הזהויות הפועלות במרחב.

זמינות - המבטיחה נגישות רציפה למרחב המקוון ולשירותים הדיגיטליים לכל שכבות האוכלוסייה והארגונים.

בטיחות וביטחון (Safety and Security) - המתייחסים להגנה מקיפה מפני איומי סייבר על תפקוד המשק, ובכלל זה על הפעולות המתבצעות במרחב הדיגיטלי, על הנכסים הדיגיטליים, ועל פרטיות המשתמשים וביטחונם, מהאזרח ועד הרמה הלאומית.

מכאן שמרחב דיגיטלי אמין, זמין ובטוח **מאפשר** את פעולת הגופים ואת מילוי ייעודם. לאור זאת, בהתאם לאסטרטגיית הסייבר הלאומית, אפשר להגדיר את **המטרה** של פעולות ההגנה בסייבר בגוף מבוקר כהשגת **אמינות, זמינות וביטחון** בנגזרת של המרחב הדיגיטלי שבה פועל הגוף, **בהתאמה** לייעודו של הגוף ולמשימותיו, **לנוכח איומי סייבר**.

סוג ייחודי של גופים המבוקרים בנושאי סייבר הם גופים אסדרתיים מדינתיים שתפקידם להנחות בתחום אבטחת המידע וההגנה בסייבר בהתאם לחוק ולהחלטות הממשלה. ההגדרה לעיל של מטרת פעולות ההגנה בסייבר בגוף מבוקר כוחה יפה גם לגופים אלה, מתוך שתי נקודות מבט: בחינת פעולתם במרחב הדיגיטלי ככל גוף מבוקר; ובחינת פעולתם בתחום הובלת ההגנה בסייבר בהתאם לייעודם ולמשימותיהם. מאמר זה לא ירחיב בנקודת המבט של ביקורת בנושאי האסדרה של גופים מסוג זה מעבר לציון כמה נושאים.

היבטים נבחנים בביקורת המדינה

כאמור, ביקורת המדינה פועלת לאיתור ליקויים ופערים ולמציאת בעיות השורש והחסמים המרכזיים לשם טיוב פעולת הגופים המבוקרים וקידום של מילוי ייעודם ושל התועלת לציבור.

כשיטה, מוגדרים שלושה סוגים של היבטים הנבחנים בביקורת המדינה:

1. היבטי ציות - Compliance Audit
2. היבטי ביצועים - Performance Audit
3. היבטים פיננסיים - Financial Audit (לא יידונו במסגרת מאמר זה)

ביקורת בהיבטי ציות מתמקדת בבחינה של הסוגיה הנבדקת **למול הנורמות** החלות עליה. בסוג זה של ביקורת בתחום ההגנה בסייבר נבדק אם פעולות הגוף המבוקר בתחום זה עומדות בנורמות החלות עליו בתחום זה, כגון תקנות הגנת הפרטיות, הנחיות מערך הסייבר הלאומי ו-ISO 27001.

ביקורת בהיבטי ביצועים מתמקדת בבחינת עמידתו של הגוף המבוקר בעקרונות של חיסכון (לא תידון במסגרת מאמר זה), **יעילות** - Efficiency (הפקת המרב מהמשאבים הזמינים) **ומועילות** - Effectiveness (עמידה ביעדים ובמטרות שהוצבו) בסוגיה הנבדקת - במקרה זה פעילות הגוף המבוקר בתחום ההגנה בסייבר.

ביקורת יכולה לשלב כמה היבטים בתוך נושא הביקורת.

נושא המאמר

מאמר זה מציג גישה בביצוע של ביקורות סייבר. מטרת הגישה היא להפיק ממצאים מדויקים ואובייקטיביים ככל האפשר על מצבם של הגופים המבוקרים בהיבטים הנבחנים, וכך לשפר את יכולת איתור הפערים המרכזיים ולתמוך במידה משופרת בתהליכי קבלת החלטות בנוגע לתעדוף הטיפול בפערים ולתקצובו. מטרה זו תושג באמצעות **מדידות כמותיות** של היבטים הנבחנים בנושא הביקורת.

---

1 משרד מבקר המדינה ונציב תלונות הציבור **מדריך לביקורת המדינה**, https://www.mevaker.gov.il/state-audit/roles-work/state-audit-guide, תפיסת ביקורת המדינה, חזון מבקר המדינה.

המאמר מסתמך, בין השאר, על תקן NIST SP 800-55v1[2], שפורסם בדצמבר 2024 ועוסק במדידת אבטחת מידע. התקן נועד להיות מדריך לפיתוח ובחירה של מדדי אבטחת מידע ברמות הארגון, המשימה והמערכת כדי לזהות את מידת הצלחתם של מסמכי מדיניות, נהלים ובקרות הקיימים בארגון בתחום.

מדידות בביקורת סייבר

בדיקות הערכה (Assessment)

חלק מההיבטים הנבחנים בביקורת מבוססים, לפעמים בהכרח, על הערכות איכותניות או הערכות כמו-כמותיות. למשל רמות נזק מפגיעה בסייבר בנכס מידע, כפי שהן מוגדרות על ידי הגוף, מבוטאות בדרך כלל בסולם של שלושה או חמישה ערכים (1 - נמוכה, 2 - בינונית, 3 - גבוהה, וכד'). בחינת יישום של גוף את ההנחיה (החוקית, האסדרתית או הרגולטורית) למיפוי נכסי מידע יכולה להיות מבוטאת גם היא בסולם של שלושה או חמישה ערכים (1 - במידה מלאה, 2 - במידה חלקית, 3 - בכלל לא וכד'). הערכות כאלה הן סובייקטיביות ופרשניות ודורשות הסכמה בין הגורמים המעורבים.

מדידה (Measurement) והערכה כמותית (Quantitative Assessment) בביקורת סייבר

מדידה בביקורת סייבר היא תהליך ההפקה של ערכים כמותיים המאפשרים להאיר - להביא למודעות - **היבט** מסוים בפעילות ההגנה בסייבר בגוף המבוקר, באופן מדויק ואובייקטיבי ככל האפשר (מובן שהיבט מסוים שנבחן הוא בהגדרתו **חלק** מתמונת מצב כוללת. יתרה מזאת, גם **אוסף** של היבטים נבחנים הוא עדיין רק חלק מתמונת מצב כוללת, בהתאמה לביקורת בכללותה, הבוחנת **נושא מסוים**).

הערכה כמותית בוחנת תוצאות של מדידה מול **קריטריון או מטרה** שנקבעו, והיא **סוג של מדידה**. אפשר למדוד, למשל, את מספר ההתרעות המתקבלות ב-SOC[3] במשך יום. אפשר לבצע הערכה כמותית של שיעור ההתרעות היומי ברמת חומרה (Severity) גבוהה (הקריטריון) וברמת חומרה בינונית ומטה.

המונח **מדד** במאמר זה יוגדר **כמהותו (תיאורו) של ההיבט הנבחן** בתהליך מדידה.

בהגדרת מדדים לביקורת סייבר יש להתייחס לשני מאפיינים:

1. המרכיבים הנבדקים - מושאי המדידה
2. סוגי המדדים

מרכיבים נבדקים בבחינת הגנה של גוף

מסמך NIST CSF 2.0 הוא מסגרת (Framework) של קווים מנחים בנושא ניהול וצמצום של סיכוני סייבר בארגון. המסגרת מארגנת את תפוקות אבטחת המידע בארגון, ברמה הגבוהה ביותר, באמצעות שש פונקציות (ראו תרשים א):

1. **משילות ארגונית - Govern**: ביסוס אסטרטגיית ניהול סיכוני סייבר בארגון
2. **זיהוי - Identify**: הבנה של הארגון את סיכוני הסייבר שלו
3. **הגנה - Protect**: יישום הגנות על נכסי המידע לצורך צמצום הסבירות (Likelihood) להתרחשות אירועי סייבר וצמצום ההשלכות (Impacts) שלהם
4. **גילוי - Detect**: זיהוי וניתוח של נסיונות תקיפה (מוצלחים או כושלים) ושל חולשות סייבר בארגון
5. **תגובה - Respond**: טיפול בנסיונות תקיפה ובחולשות סייבר שזוהו
6. **התאוששות - Recover**: חזרה לפעילות וצמצום ההשפעות של אירוע סייבר שהתרחש

המסגרת מפרטת לכל אחת מהפונקציות קטגוריות (Categories) ותת-קטגוריות (Sub-Categories) של תפוקות אבטחת מידע בארגון[4]. המסגרת גם מפנה לנורמות משלימות כגון NIST SP 800-53 (בקרות אבטחת מידע) ו- NIST SP 800-30 (מדריך לביצוע הערכת סיכוני סייבר).

---

2 NIST National Institute of Standards and Technology; - הוא מוסד ממשלתי במשרד הכלכלה של ארצות הברית המפרסם תקנים שארגונים מקצועיים ברחבי העולם מקבלים על עצמם כאמות מידה מקצועיות לתפקוד. מערך הסייבר הלאומי מקבל את תקינת NIST כתקינה מומלצת במסמכים מקצועיים שהוא מפרסם, ובכלל זה בתורת ההגנה 2.0 ובחקיקה כגון חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה - חרבות ברזל), התשפ"ד-2023.

3 Security Operations Center; SOC.

4 תורת ההגנה 2.0 של מערך הסייבר מציינת בנספח ג' את NIST CSF כבסיס להגדרת מבנה בנק הבקרות. סייבר ישראל, מערך הסייבר הלאומי **תורת ההגנה לנהל את הסיכון: המדריך היישומי (השלם) להגנת הסייבר של הארגון (תוה"ג 2.0)** (2021), https://www.gov.il/he/pages/cyber_security_methodology_2.

תרשים א: פונקציות אבטחת מידע בתקן CSF 2.0

על פי NIST CSF 2.0, תרשים 2.

מסגרת זו ונורמות מקובלות אחרות יכולות לשמש בבחירת המרכיב הנבדק שעבורו יוגדר מדד. אפשר לבחור, למשל, במרכיב **ID.RA-05** מתוך NIST CSF 2.0, שמשמעותו **שימוש של הארגון בנתוני תרחישי איום, חולשות, סבירות למימוש איומים והשלכות כדי להבין את הסיכונים ולתעדף את הצמצום שלהם** או במרכיב **PR.PS-05** מתוך NIST CSF 2.0, שמשמעותו **מניעת התקנה והרצה של תוכנה לא מורשית**.

דוגמאות למרכיבים נבדקים בגופים אסדרתיים מדינתיים בתחום ההגנה בסייבר

בגופים אסדרתיים מדינתיים בתחום ההגנה בסייבר ייגזר המרכיב הנבדק מייעודם ומהגדרת משימותיהם. בגוף אסדרתי שעם משימותיו נמנות הנחיה של גופים בתחום ההגנה בסייבר ובקרה על יישום ההנחיות אפשר, למשל, לבחון את הבקרות שעשה, לבחון את המעקב שעשה אחר תיקון ליקויים שעלו בבקרות קודמות ועוד.

סוגי המדדים

תקן NIST SP 800-55v1 מבחין בין ארבעה סוגים של מדדים:

1. מדדי יישום - Implementation
2. מדדי מועילות - Effectiveness
3. מדדי יעילות - Efficiency
4. מדדי השפעה - Impact

מדדי יישום - Implementation

מדדי יישום מראים את **ההתקדמות** ביישום של בקרות אבטחת מידע. ביישום של אמצעי למניעת הרצה והתקנה של תוכנה לא מורשית (אנטי-וירוס, EDR, XDR וכו') אפשר להגדיר, לדוגמה, מדד של מספר התחנות בארגון שעליהן מותקנת הגרסה האחרונה של תוכנת ההגנה הארגונית ביחס למספר התחנות הכולל בארגון שבהן נדרשת התקנה של אמצעי זה.

מדדי מועילות - Effectiveness

מועילות מוגדרת כעמידה ביעדים ובמטרות שהוצבו. מדדי מועילות מעריכים את **שיעור ההצלחה** של תהליכי היישום ושל בקרות אבטחת מידע במושגים של **עמידה ביעדים ובמטרות** שהוגדרו להם.

במדידה מסוג זה יש לשים לב להגדרת היעדים **והמטרות** בארגון. גוף יכול להגדיר לעצמו **יעד** של התקנת אמצעי עדכני למניעת הרצה והתקנה של תוכנה לא מורשית (אנטי-וירוס, EDR, XDR וכו') על כלל המחשבים בגוף. עמידה של הגוף ביעד זה אין משמעותה בהכרח שהושגה **המטרה** שלשמה מותקן האמצעי (כגון פעולה בטוחה של הגוף במרחב הדיגיטלי למול איום סייבר של הרצה והתקנה של תוכנה לא מורשית וחשיפה של מידע חסוי). מתוך ההבנה כי הרצה והתקנה של תוכנה לא מורשית מסכנות את חסיון המידע, אפשר בהקשר זה להגדיר מדד של השגת **המטרה** כמספר התרעות האמת התקבלו לאורך זמן ב-SIEM[5] על התקנה או פעולה של תוכנה לא מורשית בתחנות הארגון.

מדדי יעילות - Efficiency

יעילות, כאמור, מוגדרת כהפקת המרב מהמשאבים הזמינים. מדדי יעילות יבחנו היבטים כגון מהירות הפקה של תוצרים שימושיים מיישום של בקרות אבטחת מידע וכמויות של תוצרים שימושיים מיישום בקרות אבטחת מידע ביחס למשאבים המושקעים ביישומם.

דוגמה למדד יעילות יכולה להיות ממוצע הזמן להשלמת טיפול בהתרעות סייבר ב-SOC (MTTR - Mean Time To Resolve/Repair). מדד זה בוחן את משך הזמן של סך הפעילויות מרגע התרחשות אירוע, דרך הופעה של התרעות רלוונטיות ב-SOC, ניתוח ההתרעות, תיעוד ופעולות נוספות עד להשלמת הטיפול באירוע ככל שאכן היה כזה.

5 Security Information and Event Management; SIEM.

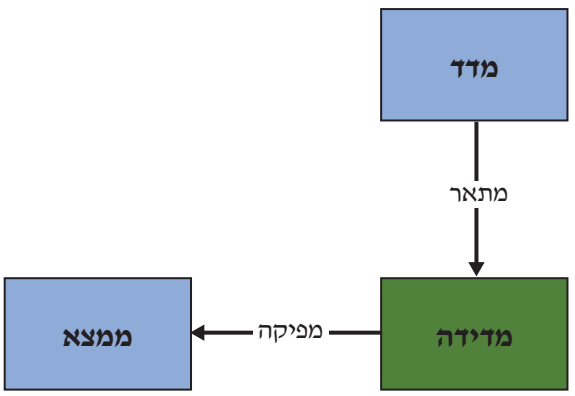
מדדי השפעה - Impact

מדדי השפעה מבטאים את ההשלכה של פערי הגנה בסייבר על מטרות הארגון, על משימותיו ועל היעדים שהוא מגדיר לעצמו. לדוגמה, בבית חולים שנמצאו בו פערי הגנה בסייבר מול תרחיש של כופרה, כגון שיעור נמוך של תחנות בארגון שבהן מותקנת התוכנה העדכנית ביותר למניעת הפעלה והתקנה של תוכנה לא מורשית, אפשר לבחון את מספר ימי ההשבתה של בתי חולים שבהם התרחשו מקרים דומים ולהעריך את העלות של מספר ימי ההשבתה הממוצע על בית החולים הנבדק.

ממצא

ממצא של **מדידה** במאמר זה יוגדר כערך כמותי אובייקטיבי המתקבל מתהליך המדידה[6] (ראו תרשים ב).

תרשים ב: יחסי גומלין בין המונחים מדידה, מדד וממצא



מידת החשיבות של ממצאים

בתהליך ביצוע הביקורת, וקל וחומר בסיכומה, יש צורך להבין את מידת החשיבות של הממצאים המסתמנים או המדדים המגובשים בתוך הנושא הכולל, זאת כהשלמה להבנת הממצאים עצמם. ביקורת תשאף לאתר את המדדים שהם מרכזיים לנושא ושבעניינם המרחק בין הרצוי למצוי של הממצאים המסתמנים הוא הגדול ביותר, ולהשקיע בהם.

גופים מבוקרים שמקבלים ממצאי ביקורת יכולים להפיק תועלת מהצגת מידת חשיבותם של הממצאים בתוך נושא הביקורת כנתונים התומכים בתהליך קבלת ההחלטות בעניין תיעדוף הטיפול בפערים והקצאת המשאבים הנדרשים.

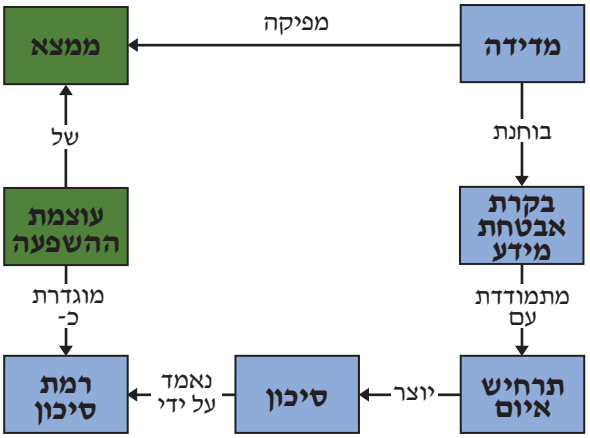
מידת החשיבות של ממצאים בתוך נושא הביקורת תוגדר **כעוצמת ההשפעה** של הממצאים על פעולת הגוף ועל מילוי ייעודו.

חישוב עוצמת ההשפעה של ממצאים

תקן NIST SP 800-55v1 מציג נושא של תיעדוף מדדים[7]. הדרך העיקרית המוצעת בתקן היא תיעדוף של מדדים באמצעות מודל סבירות והשפעה או, במלים אחרות, רמת הסיכון המוערכת לתרחיש האיום שבקרת אבטחת המידע הנמדדת נועדה להתמודד איתו. בשיטה זו נדרש להעריך (או לקבל מתוך ניתוח מאושר של תרחישי איום) את רמת הסבירות להתממשות תרחיש האיום המדובר ואת השפעתו - רמת הנזק שתיגרם לגוף בקרות התרחיש - ולשקלל אותן לרמת סיכון[8] (ראו תרשים ג, ד).

דרך זו נמצאת בהלימה עם הגדרת המטרה של פעולות ההגנה בסייבר בגוף מבוקר - כהשגת **אמינות, זמינות וביטחון** בנגזרת של המרחב הדיגיטלי שבה פועל הגוף, **בהתאמה** לייעודו של הגוף ולמשימותיו, **לנוכח איומי סייבר**.

תרשים ג: אופן חישוב עוצמת ההשפעה של ממצא

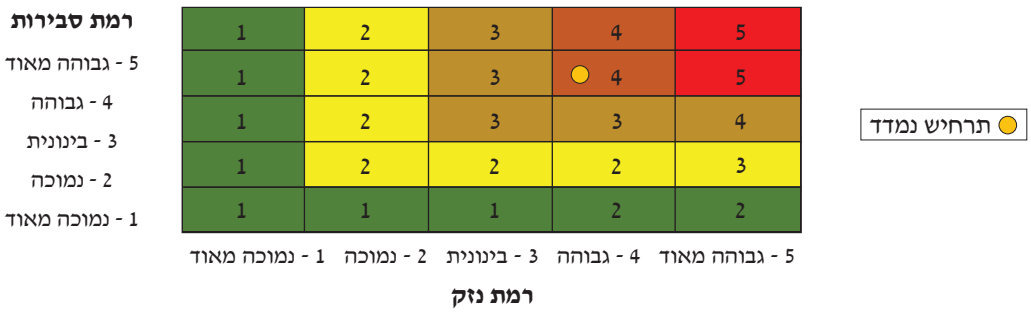


6 ייתכנו גם ממצאים של בדיקות המבוססות על הערכה. במקרה זה ממצא יהיה איכותני או כמו-כמותי.

7 סעיף 4.3 Prioritizing Measures. National Institute of Standards and Technology (NIST), Measurement Guide for Information Security: Volume 1 - Identifying and Selecting Measures (2024), https://csrc.nist.gov/pubs/sp/800/55/v1/ipd.

8 ראו בעניין זה תקן NIST SP 800-30r1, לוח I-2 National Institute of Standards and Technology (NIST), Guide for Conducting Risk Assessments (2012), https://csrc.nist.gov/pubs/sp/800/30/r1/final; סייבר ישראל, מערך הסייבר הלאומי, **תורת ההגנה לנהל את הסיכון**, לעיל ה"ש 4, בעמ' 36.

תרשים ד - דוגמה לחישוב רמות סיכון בתלות ברמת סבירות להתרחשות איום וברמת הנזק



התרשים מבוסס על NIST SP 800-30r1, לוח I-2.

למשל, למדידת מספר התרעות האמת שהתקבלו ב- SIEM לאורך זמן על התקנה או פעולה של תוכנה לא מורשית בתחנות הארגון יש זיקה ישירה לתרחיש איום של הפעלת קוד מפגע וחשיפה של מידע חסוי (וגם לתרחישים נוספים). בדוגמה זו נניח שהמדידה העלתה ממצא של מספר גבוה יחסית של התרעות, ונניח שרמת הסיכון שנותחה בגוף לתרחיש המדובר היא גבוהה, עוצמת ההשפעה של הממצא תהיה גבוהה - בהתאם לרמת הסיכון.

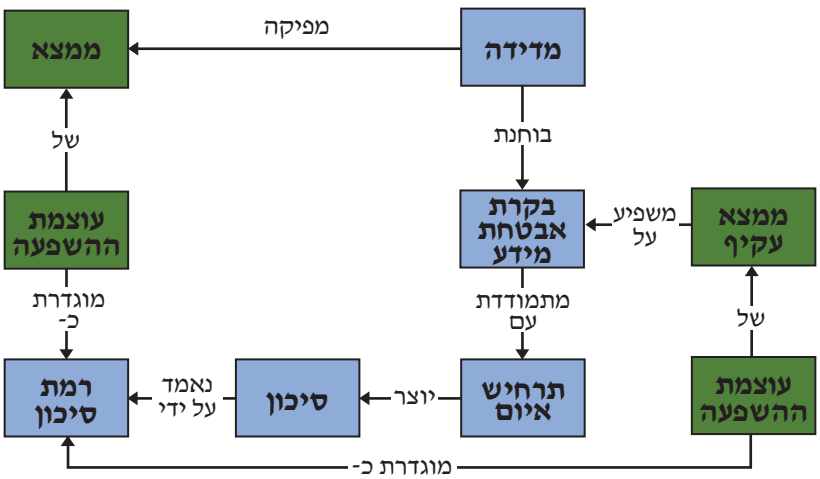
מדידת עוצמת השפעה של ממצאים בזיקה עקיפה לתרחישי איום

ממצאים של בדיקות מסוימות, כגון ממצאים של בדיקות ציות, אינם נמצאים בזיקה ישירה לתרחישי איום. ממצאים כאלה כשלעצמם לא מעידים בהכרח על פער או היעדר פער בהתמודדות עם תרחיש איום כלשהו.

במקרים כאלה רצוי לנתח ולזהות בקרות אבטחת מידע המושפעות מהממצאים העקיפים ולעשות מדידות השלמה של יישומן על ידי הגוף המבוקר. אם יימצא מתאם בין הממצאים העקיפים לממצאי מדידות ההשלמה, ואם אפשר יהיה לבסס כי הממצאים העקיפים הם גורם משמעותי לממצאים שעלו במדידות ההשלמה, אפשר יהיה להתייחס לממצאי המדידות המשלימות כבעלי זיקה ישירה, להסיק את רמת הסיכון כאמור לעיל ולשייך אותה לממצאים העקיפים (ראו תרשים ה).

נניח לדוגמה שנעשתה בדיקה של יישום ההנחיה למיפוי נכסי מידע בארגון ולסיווגם (סעיפים 6.1.3, A.8.1.1 ו- A.8.2.1 בתקן ISO27001) ונניח שהבדיקה העלתה כי נעשה מיפוי חלקי של נכסי מידע. במקרה זה אפשר לנתח ולזהות נכסי מידע שאינם מופיעים במיפוי הנכסים - למשל מחשבים ניידים של מנהלי מערכות - ולעשות בדיקת השלמה

תרשים ה: אופן מדידת עוצמת ההשפעה של ממצא עקיף



של יישום בקרות אבטחת מידע על אותם נכסים. נניח שבדיקות ההשלמה מעלות את הממצא שעל מחשבים אלה לא יושמה הבקרה של התקנת תוכנות למניעת קוד מפגע, ונניח שתרחיש האיום המשויך לבקרה זו הוא ברמת סיכון גבוהה. אפשר להניח כי היעדרם של המחשבים הניידים הללו ממיפוי הנכסים תרם במידה ניכרת לאי-יישום הנחיה מתאימה ולאי-ביצוע מעקב אחר יישום הבקרה של תוכנת ההגנה כפי שמבוצע במסגרת תהליכי ניהול אבטחת המידע בגוף. לכן עוצמת ההשפעה של הממצא העקיף בעניין מיפוי נכסי מידע היא גבוהה בהתאם לרמת הסיכון המשויכת לתרחיש האיום הרלוונטי.

אם הביקורת עשתה בדיקות השלמה ולא העלתה ממצאים המושפעים מהממצא העקיף אי אפשר לקבוע את רמת החשיבות של הממצאים העקיפים כעוצמת ההשפעה שלהם על פעולת הגוף ועל מילוי ייעודו בזמן ביצוע הביקורת. עם זאת, בדוגמה המדוברת אין להמעיט בחשיבותם של ממצאי בדיקות ציות כשלעצמם (בדגש על חוקים ורגולציות), ובפרט בהקשר של עמידת הגוף במטרות פעולות ההגנה בסייבר לאורך זמן, של שימור ההגנה בסייבר בגוף ושל ההתקדמות בנושא בעת כניסתם של בעלי תפקידים חדשים לתפקיד, בדגש על מנהלים ועל נושאים שייתכן שלא נבדקו באותה ביקורת.

היבטים של בשלות הגוף המבוקר בתחום ההגנה בסייבר

לרמת הבשלות של גוף בהיבטי הגנה בסייבר השפעה על המדידות הניתנות לביצוע.

יישום בקרות אבטחת מידע

ככלל, אי אפשר לבדוק היבטי מועילות ויעילות של בקרות אבטחת מידע שגוף אינו מיישם כלל. מתוך כך - ניתן לבצע כשלב ראשון בביקורת בדיקות ציות שמטרתן לזהות בקרות רלוונטיות שאינן מיושמות כלל, וכאמור לעיל, לבצע בדיקות משלימות הבוחנות את ההשפעה של הבקרות החסרות על פעולת הגוף ומילוי ייעודו.

יכולות מדידה

מדידות אבטחת מידע מתבססות, בין השאר, על יכולות של גוף מבוקר לשמור נתוני אבטחת מידע בעזרת אמצעים כגון קבצי לוג של מערכות אבטחת מידע (Firewall, IDS, XDR וכו'). בגופים שרמת הבשלות שלהם בתחום ההגנה בסייבר נמוכה ייתכן שלא יושמו אמצעים כאלה או שיושמו במידה חלקית, ובעקבות זאת לא יהיה אפשר לעשות מדידות מיטביות, למשל במצבים של חסר במערכות הגנה בסייבר, לוגים שאינם מכילים מידע רלוונטי ולוגים שאינם נשמרים לאורך זמן.

ערכי סף ועידן ה-AI

מהפכת ה-AI משפיעה השפעה של ממש גם על עולם ההגנה בסייבר. בין ההשפעות אפשר לציין הורדה של רף הכניסה של פושעי סייבר שבעזרת כלי AI יכולים ללא ידע מעמיק לבצע תקיפות, ומכאן לעלייה במספר התוקפים; הנגשת יכולות תקיפה מתקדמות; עליה בקצב ובמהירות של תקיפות; ושיפור ביעילות של תקיפות[9].

התפתחות זו מעלה היבט נוסף הקשור במדדים - ערכי סף. כאשר עושים מדידות כמותיות אפשר להגדיר ערכי סף המבחינים בין מצב תקין ובין פער. בלי להידרש לאופן הגדרת ערכי סף, אפשר לומר שיכולות התקיפה המבוססות על AI מקצינות את ערכי הסף. למשל, אם קצב התקיפות עולה ויעילות התקיפות עולה, מהירות התגובה להתרעות סייבר צריכה לעלות בהתאם, כך שאפשר יהיה לסכל את התקיפה בזמן.

ההתפתחות לעיל מעלה היבטים נוספים, כמו מידת היכולת של בני אדם להתמודד עם קצב התקיפות, שימוש בכלי AI להגנה כדי להתאים את קצב המענה, ומדידת היעילות והמועילות של מערכות הגנה מבוססות AI. התמודדות עם התפתחויות אלה הן חלק מאתגרי העתיד של משרד מבקר המדינה.

סיכום

לביקורת המדינה, ובפרט בהיבטי סייבר, כמה יתרונות. יתרון אחד הוא עצמאות הביקורת, האובייקטיביות שלה ואי-התלות שלה[10]. יתרון נוסף הוא הגישה של משרד מבקר המדינה לאלפי גופים מבוקרים ברמה של כלל המדינה, המאפשרת הצלבה של נתונים, ניתוח של קשרי גומלין והצגת תמונת מצב ומגמות רוחביות.

לשימוש בגישה של ביקורת מונחית מדדים יש יתרונות הן למשרד מבקר המדינה והן לגופים המבוקרים, והיא מוצגת ככלי אפשרי בביצוע ביקורות סייבר.

---

9 מאיה נחום שחל "אנחנו רגע לפני מלחמת הסייבר הראשונה שבה לא תהיה ירייה אחת" **כלכליסט** (19.11.2025) calcalist.co.il/conferences/article/ryhca0fgbx.

10 משרד מבקר המדינה ונציב תלונות הציבור **מדריך לביקורת המדינה**, לעיל ה"ש 1, תפיסת ביקורת המדינה, עקרונות הליבה https://www.mevaker.gov.il/state-audit/roles-work/state-audit-guide.