stki.info
IT Knowledge Integrators
Moshav Bnei Zion P.O.Box 151, 60910 Israel Tel. 972-9-7907000 Fax. 972-97442444

# נייר עמדה

# מבנה ארגוני וקבלת החלטות בתחום סייבר בארגוני Enterprise IT

גרסה: 1

פיני כהן

נייר עמדה: מבנה ארגוני וקבלת החלטות בתחום סייבר בארגוני Enterprise IT

סיכום מנהלים:

- בתחום הסייבר יש להבחין בין "**גורם מבקר**", "**גורם מנחה**" ו"**גורם מתפעל**" (אחראי סייבר).
- הגורם האחראי לטיפול ותפעול נושא הסייבר בארגון הוא ה-CIO ("**הגורם המתפעל**"). **לא ניתן להפריד בין תפעול ה- IT הכללי לבין תפעול נושא הסייבר**.
- לעיתים, יאציל ה- CIO סמכות (ואחריות) לטיפול ותפעול נושא הסייבר למנהל התפעול-תשתיות.
- יש להקים **צוות סייבר תפעולי** (צוות סייבר) שיהווה **"הגורם המתפעל"** בפועל. מדובר על צוות רב תחומי תפעולי תחת האחראי על נושא הסייבר בארגון. גורם זה יטפל בפועל באירועי סייבר, יתפעל כלי סייבר יעודים, יפעל למניעה של אירועי סייבר, יתעדכן לגבי התקפות ופגיעויות רלוונטיות לארגון, וינחה תפעולית את ה- IT בנושא סייבר. גוף זה יעבוד בצמידות לגוף התפעול והתשתיות בארגון.
- **הנחייה, יישום רגולציה והחלטה בנושאי סדר עדיפויות** בתחום סייבר צריכה להיעשות באופן ממוקד על ידי **"גורם מנחה"**. גוף זה יכול להיות תחת הגורם המתפעל או **מחוץ ל- IT** (תחת אחראי סיכונים ארגוני, CFO, בטחון, אחראי רגולציה וכד'). גוף זה יעבוד בצמידות ל"גורם המתפעל".
- **על הנהלת הארגון הבכירה ביותר** להתייחס לנושא הסייבר כולל קבלת החלטות מהותיות, קביעת סדר עדיפויות ותקצוב. יש לבנות תהליך ארגוני המאפשר התייחסות זו. ריכוז תהליך זה באחריות **"הגורם המנחה"** ו- **"הגורם המתפעל"**.
- במקביל לגורם המתפעל והמנחה יש להקים **גורם מבקר** שהנו בלתי תלוי (גם לא בגורם המנחה). גורם זה יבקר באופן מעשי את פעילות הגורם המתפעל ואת מוכנות הארגון לאירועי סייבר (ביצוע PT ומבחנים אחרים).

**תוכן:**

פתח דבר .....3
מה בעייתי כל כך בתחום סייבר לעומת תחומים אחרים ב- IT? .....4
השפעת ה"רב תחומיות" על חלוקת האחריות בנושא סייבר .....5
צוות סייבר תפעולי .....5
אופן פעולת צוות הסייבר.....6
מיקום ארגוני של צוות הסייבר .....6
ריחו של הדג .....6
הפרדת הגורם המבקר משאר הגורמים .....7
גורם מנחה, רגולציה, קביעת מדיניות ובניית מטריצת איומים .....8
רמת הפירוט של ההנחיות ושל מטריצת האיומים .....9
אחריות על נושא מודעות סייבר .....9
נקודות כשל .....10

## פתח דבר

נושא הסייבר תופס חשיבות גדולה יותר ויותר בקרב ארגוני Enterprise IT. חלוקת האחריות וקביעת חלוקת הפעילות בתחום זה הנם מורכבים ומצריכים מחשבה.

מטרת מסמך זה הנה להתוות את מערכת היחסים, שיטת הפעולה והמבנה הארגוני בתחום סייבר בקרב ארגוני Enterprise IT.

בשוק ישנן הגדרות שונות לנושא "סייבר" ולנושא "אבטחת מידע". במסמך זה אנחנו מתייחסים לשני המונחים כאחד ומכוונים להגדרה הרחבה ביותר של התחום על פי הפרספקטיבה של Enterprise IT.

בשוק מקובל השימוש בתואר CISO – chief information security officer. במסמך זה בחרנו שלא להתייחס למונח זה כי לעיתים הכוונה ב- CISO ל"גורם מנחה" , לעיתים כ"גורם מבקר" ולעיתים גם כ"גורם המבצע" (מנהל צוות סייבר).

מסמך זה פורש את חלוקת התפקידים והאחריות המומלצת - המיטבית. חלוקה זו עשויה להראות מסורבלת ויקרה לארגונים שאינם גדולים ואשר אינם יכולים להקצות מספיק בעלי תפקידים ומשאבים. ארגונים יכולים לאחד כמה תחומי אחריות תחת גורם אחד. יש לנסות

ולהקפיד לא לאחד תפקידים מרמות אחריות שונות – לדוגמה אחריות של דרג מבקר ביחד עם אחריות של דרג מתפעל.

במסמך זה לא התייחסנו לסוגיה של מיקור חוץ בתחום הסייבר שהנה פרקטיקה מקובלת במקרים מסוימים. ניתן להוציא חלק מהתפקידים שהצגנו כאן למיקור חוץ.

## מה בעייתי כל כך בתחום סייבר לעומת תחומים אחרים ב- IT?

תחום הסייבר מאופיין בשילוב של מספר מאפיינים ייחודיים לעומת תחומי IT "רגילים":

1. תחום הסייבר הנו בהגדרה רב- תחומי. אמנם ישנם אזורי סייבר ספציפיים – תחום רשת, תחום שרתים, תחום תחנות קצה, תחום פיתוח, תחום מסדי נתונים ועוד. אבל ראיית התמונה הכוללת שמשמעותה יכולת להתמודד עם APT שלדוגמה פנה לארגון באמצעות social engineering ולאחר מכן ביצע הפניה וחדירה דרך גלישה –WEB, לאחר מכן השיג נתוני משתמש משרת, ולאחר מכן ניגש למסד נתונים וביצע בו פעולות וכד' –כל אלה מחייבים רב תחומיות ויידע ייחודי וייעודי שמתעדכן כל הזמן.
2. זהו תחום מונחה רגולציה "כבדה" במגזרים מסוימים. רגולציה בתחום הסייבר מחייבת התמחות (מה מקובל, מה המשמעות והאלטרנטיבות, כיצד התייחסה רגולציה לצעדים שיזמו אחרים בשוק וכד').
3. לכאורה, זהו תחום שבו יש ניגוד אינטרסים מובנה בתוך ה- IT. אנשי התפעול מעוניינים לספק את הזמינות הגבוהה ביותר. זאת בניגוד לאנשי הסייבר המעוניינים לוודא שלא מתרחש אירוע סייבר ושמירב הכלים והתהליכים מוטמעים בכדי למנוע אירוע זה. דוגמאות ל"התנגשות" בין אינטרסים אלו – כאשר יש תקלה, ה- IT רוצה להעלות את המערכות כמה שיותר מהר. הסייבר רוצה לבצע שימור ראיות (dump) של הסביבה (מה שלוקח זמן) בכדי שיוכל לתחקר מה אירע ברמת סייבר. דוגמה נוספת, AGENT של סייבר גורם להאטת ביצועים כאשר מצד אחד יש רצון להפסיק ולהשתמש בו עקב האטת הביצועים, מצד שני נשאלת השאלה כיצד לאתר המידע החיוני בהקשר סייבר.
4. תחום בו ההתפתחויות הטכנולוגיות מתרחשות בקצב מהיר במיוחד.
5. תחום בו התפעול היום יומי קשור לאזורים שנמצאים מחוץ לארגון. כלומר, מדובר על תחום בו חשיבות ההתעדכנות רבה יחסית. בניגוד לתחומי ה- IT האחרים (ERP, אחסון) בהן הקשר לאזורים שנמצא מחוץ לארגון (כלומר התעדכנות) הנו חשוב אך לא באופן מיידי (לדוגמה, קבלת מידע על עדכון ב- ERP הנה חשובה אך יכולה להתרחש בתדירות של שבועות) הרי שבתחום הסייבר החיבור למה שקורה מחוץ לארגון חייב להיות יום יומי.
6. ההשקעה בתחום הסייבר נתפסת כסוג של ביטוח שהנו "הוצאה הכרחית" שאינה תורמת לשיפור המהלך העסקי של הארגון. כי במצב "נורמלי" אין ארועי סייבר ואז נראה שתקציב הסייבר הנו "בזבוז".

עם זאת, יש לציין שרוב מאפיינים אלו קיימים ב- IT במידה כזו או אחרת. רגולציה קיימת גם שלא בהקשר לסייבר. רב תחומיות כבר קיימת כי לדוגמה ביצוע vmotion (תחום סיסטם) מחייב הבנה הן של תשתית הרשת והן של האפליקציה. לגבי ניגוד אינטרסים ודילמות הדבר מובנה בכל תפקיד ניהולי – משמעות העלאת פרויקט לאוויר בזמן לעומת ביצוע בדיקות באופן מלא. תעדוף של שדרוג מארז אחסון ישן שעלול לגרום לתקלות למול מעבר לטכנולוגיה חדשה שתאפשר ייעול השירות ל-business וכד'. גם ההשקעה בסייבר כסוג של ביטוח קיימת בתחומים אחרים (גיבוי, DR, בדיקות תוכנה וכד').

## השפעת ה"רב תחומיות" על חלוקת האחריות בנושא סייבר

### צוות סייבר תפעולי

מכיוון שתחום הסייבר מחייב בניית ידע והתמחות ייחודית, יש לבנות צוות סייבר תפעולי ייעודי. לעיתים נקרא לצוות זה "צוות סייבר" בלי להזכיר את המילה "תפעולי". צוות שמתמחה בעולם הסייבר – מתפעל, לומד, מתעדכן ומתרגל. החלק המקצועי ביותר בצוות זה מוגדר לעיתים כגוף אנליסטים.

צוות זה גם יתפעל כלי סייבר יעודיים, יהיה אחראי על מרכז הבקרה בנושא סייבר (SOC) וגם ינחה גופים בתשתיות, בפיתוח ובתפעול ב- IT. כלומר ינחה את גוף ה- PC, גוף ה- DBA, המפתחים ולמעשה כולם במה צריך לעשות ולעיתים גם "איך מומלץ לעשות". בשעת אירוע סייבר צוות זה יתפעל את האירוע בהקשר הפנימי. לעיתים צוותים אחרים יסייעו לצוות הסייבר בתפעול אירוע סייבר בהקשרים חיצוניים (דיווח להנהלה, דיווח לרגולטור וכד'). לעיתים הגוף המנחה הוא המסייע בתפעול אירועי סייבר בהקשר החיצוני (הנהלה, וכד').

בארגונים גדולים צוות הסייבר יתחלק למספר חוליות:

- אנליסטים – בעלי הידע התפעולי הרב ביותר. הם יטפלו באירועי סייבר, יעדכנו את חוקי ה- SIEM , ינחו את צוות ה- SOC
- צוות ה- SOC
- חוליית הנחייה – המנחה מעשית את כל בעלי המקצוע בארגון בתחום סייבר (הנחייה של פיתוח, DBA , רשת, PC וכד').
- חוליית תפעול כלי סייבר ייעודיים (כלי חקירה, ניטור תעבורה, כלי deception וכד'). ניתן לשקול מצב בו כלים תשתיתיים שהנם בעלי משקל גבוה בהקשר סייבר (FW, כלי הגנה של DBMS, כלי סקירת קוד סטטי ודינאמי וכד') יטופלו גם הם על ידי צוות הסייבר.

### אופן פעולת צוות הסייבר

מכיוון שנושא הסייבר הנו רב תחומי, גם טיפול באירועי סייבר מחייב פעולה רב תחומית. פעולות בכלים שמוגדרים ככלי סייבר ובמקביל פעולות בכלים שאינם מוגדרים ככלי סייבר (שרתים, תקשורת, DBMS PC קוד וכד'). המשמעות היא שצוות הסייבר הייעודי (כולל האנליסטים) יהיו חלק מגוף התשתיות-תפעול, שותפים בהעברות לייצור ובפעולות אחרות ב-IT בכדי שיכירו את האנשים-תהליכים-מערכות –פרויקטים באופן צמוד. לא ניתן להפריד את צוות תפעול הסייבר משאר צוותי תפעול ה- IT בארגון. זוהי הסיבה שהאחראי על תפעול נושא הסייבר – ולכן גם הגורם האחראי על תחום הסייבר באופן כללי, הוא ה- CIO. ה- CIO יכול לקבל הנחיות בנושא סייבר מגורמים אחרים בארגון (בהמשך ישנו פרק שמדבר על נושא הנחייה). כמו כן צריכה להיות בקרה על ה- CIO בהקשר לתפקודו בתחום הסייבר על ידי גורם חיצוני (בהמשך ישנו פרק שמדבר על נושא בקרה). אך האחריות על תפעול נושא הסייבר נמצאת על כתפיו של ה- CIO.

## מיקום ארגוני של צוות הסייבר

כאמור, האחראי על נושא הסייבר בארגון הוא ה- CIO. לעיתים מאציל ה- CIO את הסמכות (והאחריות) על נושא הסייבר למנהל התפעול\תשתיות. ואז נשאלת השאלה איפה נמצא צוות הסייבר התפעולי. האם תחת מנהל התפעול\תשתיות או במקביל אליו (מתחת ל- CIO)? התשובה כאן היא "כל הדרכים מובילות לרומא – אבל רק הדרכים הנכונות". העיקרון המנחה כאן הוא שגם אם צוות הסייבר לא נמצא מתחת למנהל התפעול\תשתיות עליו לתפקד באופן אינטגרלי וצמוד לתפעול\תשתיות. שני הצוותים, צוות הסייבר וצוות התפעול\תשתיות הכללי, צריכים לעבוד כמקשה אחת. על צוות הסייבר להיות מודע לאנשים, לתהליכים, לפרויקטים חדשים ואפילו לנושאים כמו רכש ולכל מה שמתרחש בתפעול\תשתיות. במיוחד עליו להיות חלק מתהליך ההעברה לייצור, זאת בכדי שבזמן אירוע סייבר כל המערכת התפעולית תתפקד כארגון אחד.

## ריחו של הדג

בדיון דובר על תופעה שבה הגורמים התפעוליים (בעיקר גורמי תשתיות אבל גם גורמים אפליקטיביים) לא ששים לבצע משימות אבטחת מידע. זאת מן הטעם שהם יותר מחוברים למשימות הראשיות שלהם – הן אם מדובר על פיתוח והן עם מדובר על זמינות מערכות בתשתיות – ולכן לא תמיד מבצעים במלואן הנחיות שמתקבלות מהגורם המנחה בתחום

אבטחת המידע. במקרים מסוימים ישנה תחושה שלגורם המנחה בתחום אבטחת מידע אין מספיק "שיניים".

הערת STKI – בעיות ניהוליות תמיד קיימות אולם יש לפתור אותן באמצעות כלים ניהוליים: הגדרת משימות סייבר בתוך תכנית העבודה של כל הגורמים, מעקב אחרי התקדמות תכנית העבודה וגילום ביצועי העובדים והמנהלים בשיחות הערכה ובסופו של דבר בקידומם. או במילים אחרות, כידוע הדג "מריח טוב מהראש וגם מסריח מהראש" – הכל תלוי בתרבות הניהולית של ה- CIO.

## הפרדת הגורם המבקר משאר הגורמים

אחד מרכיבי תכנית הסייבר בארגון הוא ביצוע בקרה. מדובר בעיקר על ביצוע PT וסקרי סיכונים. בקרה נוספת היא שתהליכים אכן מתבצעים, מוצרים אכן מיושמים כראוי וכד'. בקרה נוספת היא בקרה על רמת הערנות והמודעות בארגון בנושא זה.

רמה זו צריכה להיות מופרדת משאר הדרגים שמטפלים בסייבר. הן מרמת אחראי על הסייבר (שהוא מתפעל הסייבר) והן מרמת קובע המדיניות, ההחלטות ותעדוף בסייבר (על כך בהמשך). לא ייתכן שהגורם שמיישם את מדיניות הסייבר יבדוק את עצמו. כמו כן, לא ייתכן שהגורם שמנחה את מדיניות הסייבר, קובע סדרי עדיפויות ומתקצב את פעולות הסייבר יבדוק את עצמו (כי באופן "טבעי" לא יפנה משאבי בחינה לאזורים אותם לא הנחה לבצע).

בארגון אידאלי שבו אין מגבלה תקציבית ניתן היה לחשוב על כמה רמות או כמה מעגלים של בחינה. רמת בחינה אחת היא של הדרג המנחה – בקרה שההנחיות שלו התבצעו. רמה נוספת של הדרג המבצע שבה הוא מבצע בחינת סייבר (PT וסקרי סיכונים) לפני שהוא מעביר מערכות לייצור (במיוחד כאשר מדובר על פיתוחים או חבילות שנרכשות מגורמים חיצוניים). אך במקביל, בלי קשר לבדיקות אלו, גם הגורם המבקר יכול לבצע בחינה לפני המעבר לייצור או כאשר כבר המערכת בייצור. ברוב הארגונים הדבר אינו אפשרי ולכן אם רוצים להשיג רמה גבוהה יותר של מוכנות בתחום סייבר, הגורם הבוחן צריך להיות מופרד מאשר הגורמים. ניתן גם לחשוב על מספר מעגלים של בקרה. מעגל ראשון של הגורם המתפעל או מנחה. מעגל שני של צוות בקרה בתחום סייבר- לעיתים יכול לשבת בגוף האחראי על רגולציה בארגון. ומעגל שלישי – גוף הביקורת של הארגון.

הגורם המבקר יכול לקבל זכויות צפייה (read only) בכל כלי הסייבר.

## גורם מנחה, רגולציה, קביעת מדיניות ובניית מטריצת איומים

הנחיות רגולטור הנם אחד הגורמים המשפיעים ביותר על יישום תחום הסייבר בארגונים בתעשיות השונות. הגורם המנחה אמון על דרישות הרגולציה, על שינויים צפויים ברגולציה ועל תרגומן ספציפית לארגון. בנוסף לכך, אחד הפקטורים החשובים ביותר להתמודדות עם נושאי הסייבר הוא קיומה של מטריצת איומים \ פתרונות עדכנית בארגון הקובעת את מדיניות הסייבר בארגון, סדרי העדיפויות ואת תכנית העבודה בתחום זה. מכיוון שלא ניתן למנוע את כל הסוגים של מתקפות הסייבר וליישם את כל הפתרונות האפשריים אשר יתנו ערך מוסף, ארגון חייב להסביר לעצמו (ולעיתים גם לאחרים) מדוע הוחלט לטפל בנושא אחד ולא בנושא אחר. מטריצה זו צריכה להיות מאושרת לפחות פעם בשנה על ידי הנהלת הארגון הבכירה ביותר וצריכה להיות מעודכנת במהלך כל השנה. זאת מכיוון שאיומי הסייבר משתנים וגם מבדקים (PT סקר סיכונים, תוצאות סקר ערנות וכד') עשויים לשנות את המטריצה במהלך השנה. מדובר על תהליך שמחייב התמחות מקצועית בנושא של ניהול סיכונים ובנוסף בתחום סייבר ולכן רצוי שיהיה בארגון גורם ספצפי שאחראי על נושא זה, אמון על תחום ניהול הסיכונים, רגולציה ובעל ידע מתאים המחובר למתרחש בארגון (ומחוץ לארגון) בתחום הסייבר (מודע לאירועי סייבר בארגון ומחוצה לו, מקבל מידע של cyber intelligence , מגמות בתחום סייבר וכד'). עדיף שגוף זה לא יהיה "הגורם המתפעל" מכיוון שהגורמים המתפעלים עמוסים ולא יכולים "להרים את הראש מעל המים". כמו כן, לגורמים המתפעלים יש בדרך כלל פחות ידע מתודולוגי בנושא ניהול הסיכונים וברגולציה.

גורם זה יימצא בתוך ה- IT (אך בנפרד מגוף התפעול) או בתוך הביטחון, CFO, רגולציה, ניהול סיכונים ארגוני וכד'.

למרות שגוף זה נפרד מגוף התפעול חשובה ביותר הסינרגיה בין גופים אלו בכדי שההנחיות, תוכנת הפעולה והמדיניות יהיו ישימים לביצוע בארגון.

הגורם המנחה יכול לקבל זכויות צפייה (read only) בכל כלי הסייבר.

ניתן לשקול מצב בו הדרג המנחה גם מבצע בקרה על כך שההנחיות שלו בוצעו.

## רמת הפירוט של ההנחיות ושל מטריצת האיומים

כאמור ישנו גוף אשר נותן הנחיות, קובע מדיניות וקובע את תכנית העבודה בתחום הסייבר (הנגזרת ממטריצת האיומים). נשאלת שאלה באיזו רמה של פירוט מתקבלות ההנחיות.
ניתן כאן דוגמה לדו-שיח אופציונלי בין הגורם המנחה לגורם המתפעל-מיישם:

- "נא ליישם עקרונות אבטחה כלליים ונהלים אלו...".
- "נא ליישם דרישות אבטחה אלו לצורך עמידה ברגולציה X ..."
- "נא לטפל בממצאי PT (או איומים חדשים) אלו..."
- "נא לטפל בממצאי PT אלו באמצעות סוג טכנולוגיה זו ..."
- "נא לטפל בממצאי PT אלו באמצעות אחד מכלים אלו ....".
- "נא לטפל בממצאי PT אלו באמצעות מוצר X....."
- "נא לסגור פורט X ולשנות תהליך תפעולי Y....".

על פי העקרונות אותם תיארנו כאן, דרך הפעולה המועדפת היא שהגוף המנחה קובע את ה"מה" והגוף המתפעל קובע את ה"איך". כלומר, דו-שיח של "נא לטפל בממצאי PT (או איומים חדשים) אלו..." והגוף המתפעל קובע באמצעות איזו טכנולוגיה, איזו מוצר וכיצד ליישם את המוצר.
ישנם מקרים שבהם הנחייה של הגורם המנחה תהיה מלווה בתוספת תקציב לגורם המיישם. המצב הרצוי הנו שהגורם המנחה מוציא את הבקשה\הנחייה והגורם המתפעל משתף את הגורם המנחה בתהליך הבחירה.

## אחריות על נושא מודעות סייבר

ברובם המכריע של הפריצות החמורות ישנה מעורבות של גורם אנושי שהנה נקודת הכשל הראשונית. ולכן חשיבות הנושא של מודעות וחינוך בתחום סייבר קיבלה בשנים האחרונות דחיפה גדולה. המצב האידאלי הוא שעובדי הארגון מתורגלים כל השנה בנושא זה (כולל פעולות אנושיות "אנחנו מדברים מה-IT – אתה מתבקש למסור לנו את הסיסמא") כאשר תוצאות הבחינה משתלבות במנגנון של הערכת העובדים.
במצב אידאלי הינו מצפים שתחום כ"א \ הדרכה יקבל אחריות על נושא המודעות (עם סיוע של הגורם המתפעל בתחום סייבר) כאשר במקביל לתוכנית המודעות שתחום ההדרכה\כ"א מפעיל, הגורם המנחה מבצע בדיקות מטעמו בכדי לוודא שרמת המודעות אכן השתפרה.

אולם במקרים רבים אנחנו רואים שהגורם המבקר אחראי לתוכנית המודעות וגם לבקרתה, וצריך לפחות להיות מודעים לחסרון שבכך.

## נקודות כשל

נתאר כאן מספר נקודות כשל אופייניות בהקשר חלוקת אחריות בנושא סייבר אליהן יש לתת את הדעת:

- גופי הפיתוח והתפעול\תשתיות לא מיישמים הנחיות בתחום סייבר מחוסר מודעות וניהול תקין
- גופי התפעול\תשתיות והפיתוח עמוסים לכן ולא נותנים מספיק עדיפות למשימות סייבר (על חשבון משימות זמינות או פיתוח). טיפל בתקלות מתבצע בראייה של "זמינות" ולא של סייבר. כלומר גופים עמוסים לא מספיק מקצועיים בנושאי סייבר ולכן עושים טעויות.
- צוות הסייבר התפעולי אינו מחובר למתרחש בארגון ובשעת אירוע לא מכיר את האנשים\המערכות וכד'.
- אין מספיק תרגול של אירועי סייבר בארגון.
- גוף ההנחיה "מנחית דברים" שאינם מחוברים לשטח וללא תקצוב ראוי.
- ההנהלה הבכירה אינה מודעת למוכנות הארגון בנושא סייבר.

ארגונים צריכים לשים לב שאינם נופלים ל"מלכודות" אותן הזכרנו (ישנן מלכודות נוספות) ובמידה וכן מתגלה כשל לבצע מהלכים מתקנים בהתאם.