CISO Track TLV 2020 - Event Proceedings

נכתב על ידי רעות מנשה 30.06.2020

נערך על ידי יפתח איאן עמית

מסמך זה מסכם את הדיונים שנערכו באירוע המקצועי בדלתיים סגורות. המסמך מתקצר את הדיונים ולא כולל את כל האמירות והנתונים שהועלו. המסמך נכתב בלשון זכר, גם כאשר מתייחסים למשתתפות בדיון - וזאת על מנת לשמור על כללי האירוע בהן לא ניתן לייחס אמירה מסוימת לאדם.
המסמך מנוסח בסגנון המשלב סיכום של נקודות דיון וכן אמירות כלליות על ידי המשתתפים.

נושא 1: cloud security

מציג תחום הבעיה: אריק גומורובסקי מ-ermetic.
בתחילת הדרך, כולם דיברו על הנושא של אבטחת מידע בענן אבל אף אחד לא באמת עושה את זה. כל הנושא של traditional operations משתנה. אחריות ה - it עוברת למפתח ול - devops.
ה - cio מתחיל לחפש את עצמו, כי האחריות עברה לגוף ה - engineering.
בהקשר הזה, גם ארגוני ה - ciso עוברים שינוי.

נקודות לדיון:

1. מי אחראי לשמור על סביבת ה - public cloud infrastructure כסביבה מאובטחת, האם זה אצל הסיסו, בפיתוח, או בהנדסה?
2. איך התהליכים נראים ?
    a. מי אחראי על ה - policy ? מי אחראי על ההטמעה ? מי אחראי על ניטור ?
    b. נושא ה - iam - מה התהליכים הקשורים לזה ומי אחראי לכל תהליך ?
3. מקרי בוחן מעניינים לשיחה:
    a. אבטחת רשת וקונפיגורציה
    b. iam
    c. קונפיגורציות אבטחה כלליות (ויזבליות)

דיון:
אם פעם סיסו היה מתעסק עם פיירולים ורשתות, אנשי סקיוריטי היו מתעסקים בימים ההם ברמה הגבוהה מאוד, בנהלים בעיקר, לא באמת היו מתעסקים עם הברזלים. היום בעולם הענן, הציפייה, להבנת אחד המשתתפים והצוות שלו, היא שהם חלק מהשטח, הם חיים בשוחות, הם מקנפגים, הם בונים, הם כותבים את הjsonים של הiam. כי זאת הציפייה. זה כבר לא כמו פעם. הציפייה השתנתה כלפי צוותי ה - security. גם ה - devops עצמו מצפה שיעשו את העבודה עצמה ולא רק ינחו אותם. זה חלק מההבנה ש - security הוא לא ילד מיוחד, ברגע שאתה אחד מהצוות, הציפייה שתדע לעשות את הדברים האילו ביחד איתם. אנשי הסקיוריטי יושבים כחלק מצוות הפיתוח, הכל מגיע מההבנה שה - security הוא חלק מה - design. הם בנו

את הדברים, הם מכירים. הם לא שמעו על זה מרחוק. השיחה בעקבות כך משתנה לגמרי. פידבק הוא בהתאם.
משתתפים נוספים מסכימים שזו הגישה והכיוון האידיאלי, אך ברוב המקרים זה לא המצב שכן בחברות רבות יש יותר מתח בין צוותי הפיתוח לאנשי הסקיוריטי, ובמקרים רבים הסיסו לא מקבל/לוקח מספיק אחריות על ה-hands on.

מהות תפקיד הסיסו ? הרבה מהחברות רוצות פשוט שקט מה - security, יש כאלו שנשארים בגישה של נותנים הוראות ולא כל כך אכפת להם איך הם ממשים את זה. מעט מאוד עשו את הטרנספורמציה לצוות שהוא תפעולי יותר. ויש גם יחידות שעדיין שומרות על מרחק מאנשי ה - security ולא תמיד יש את החיבור בין הצוותים. בין ה - devops ל - security למרות שאנשי ה - devops היו מאוד רוצים שיקחו מהם את הנושאים הקשים.

האם יש ציפיה שה - ciso ידע את הכל? גם אם הסיסו לא יודעת את הכל. הציפייה שהסיסו יביא לשולחן את האנשים שיעזרו לו לעשות את הדברים האילו לרתום את הארגון לעשות את הדברים האילו.

בדיון עולות שאלות לגבי scaling של סקיוריטי, שכן בחברות גדולות לא ניתן (ואין ציפיה) לשמור על יחס גבוה יחסית בין כמות אנשי הסקיוריטי למפתחים. איפה נכנסת פונקצית הגדילה כשעוברים מחברה קטנה/בינונית לחברה דגולה? אולי ב-security champions? בהטמעת כלים יותר יעילים (בין אם על ידי gating functions, הנחיות או היזון חוזר קרוב יותר למפתחים)?

צריך לדעת להיות על כל הספקטרום ומתי הטיימינג המתאים. הגישה של ה - champion היא גרועה לדעת אחד המשתתפים, זה דומה לנע״ת בצבא. אם כולם מבינים שכל אחד ביום יום שלהם מתעסקים עם ה - security ולא זורקים את האחריות על ה - champion רק אז אפשר באמת להתרחב.

אחד המשתתפים שיתף את הגישה של לחלק את הדברים בצורה פרויקטאלית - יש דברים שבהם עובדים כטייס ודברים בהם לוקחים את תפקיד הנווט. לדעת להגיד בדיוק איפה רוצים שזה יהיה, מה ההגדרות, מה ה policy איך בונים תוכנית פריסה. דברים שלכאורה production אמורים לדעת לעשות. אם יש לי ערך מוסף אז קל לתת לי להוביל. זה לא אומר שהסיסו צריך להגדיר אתה - terraform.

עולם ה - cloud הביא יכולות של הרבה דברים. פעם היינו הולכים ל data center ואומרים לו תביא לי את כל traffic וזה בהחלט היה דבר מוזר וארוך. היום בלחיצת כפתור יש audit trail, הכל ב - api. זה עולם אחר לגמרי.והיום גם לא צריך אותם, אתה יכול לבד.

בסביבת ענן מודרנית המעבר ממודלים ישנים יותר של ניהול הרשאות וזהויות הופך למסובך באופן מעריכי. יש שרשור של רולים, בקצה של אחד הרולים יש *.s3 שיכול למחוק לך את כל ה - s3. אותו דבר בעולמות ה - sass, אתה כבר לא צריך להרים את התשתיות אבל מצד שני יש לך 200 saasים בארגון ולך תשתלט על האירוע הזה, ה - sf הכל בסדר איתו אבל חיברו לי שם איזה מוצר ששואב לי את כל ה -sf ואני אפילו לא ידעתי על קיומו.
אחד המשתתפים העיד כי יש לו 200 כאלה אפליקציות המחוברות ל-sf.
עם כל זאת, המשתתפים הסכימו שהם רואים הרבה יותר יתרונות בעולם ה - cloud מאשר חסרונות. בעולם של השותפות אנחנו לוקחים את האחריות ביחד עם אנשי הפרודקשיין, יש מקומות שבהם אני למעלה וחלק מהם אני למטה,

אחד המשתתפים שיתף שאנחנו מדברים על לגייס cio, אבל זה תפקיד אחרי לחלוטין, המצאנו תפקיד, לכל אחד יש תהליך הכנסת מערכות והיינו רוצים שנעשה שיקול ביזנס האם להכניס מערכת או לא. שמישהו ינהל את התהליכים ואת ה - data flow. והוא לא קשור ל engineering והוא נטו bussiness function. אז זאת הפונקציה שהיא נטו ביזנס ושמישהו ינהל את זה ברמה הארגונית.

נושא 2 - Optimizing Operational Security

מציג תחום הבעיה: מיכאל מומקואגלו מ-cardinal ops

עולם ה-security operations הוא מסובך, וזה הולך ונהיה מסובך יותר ככל שיש יותר מוצרים המשתלבים במשימה. יש המון אתגרים ולכל אתגר יש מוצר, ואפילו התועלת הולכת ונהיית שלילית.

המשתתפים מעירים כי הנושא של misconfiguration. זאת תפיסה גרועה של ונדורים. המטרה שלי בתור ונדור שהלקוח ינצל את המקסימום של המוצר שלי, אם הוא לא זאת תקלה. ל - csmים שלנו אין קוואטות, הם אמורים לראות שהלקוח מנצל את מה שהוא קנה בצורה הכי טובה שיכולה להיות.

מיכאל: הטייטל אופטימייזין הוא מאוד מעניין, מה אנחנו מנסים לעשות ? אנחנו מנסים להיות יותר יעילים ? יותר חסכוניים? ורציתי לשאול את הפורום, כמה ארגונים יש פה טיקטים של security ולא מטפלים בהם באופן קבוע.

הדיון מתחיל בהבנה של למה קוראים ticket והכרה בכך שלא כל ה-tickets נולדו שווים, וכחלק מכך זה בסדר שחלקם לא מטופלים, או מטופלים בעדיפות נמוכה.
יש incident שהוא אירוע שהוא מחוץ לסקופ של האנליסט tier 1 כנראה שאתה מערב בו הרבה אנשים. כמה אירועים כאלו יש ? אם אתה מייצר אוטומציה מסודרת אז הפחד לאבד דברים הוא יורד עד האירוע שהוא שולי נורא.
הגישה של הרבה socים היתה שמכיוון שבוחנים אותם על היכולת לאתר את צוותי ה-pentesting הם צריכים להגדיל את כיסוי ה-logים שלהם. זה יצר מצב שבו יש המון לוגים, אבל לא נעשתה עבודת fine tuning ויש המון התראות, מה שיצר גישה שבכל מקרה הכל false positive וחוזרים לנקודת ההתחלה שמרוב לוגים לא רואים את ההתקפות.
התפתח דיון על כך שה-soc המודרני הוא לא חדר עם מסכים ומפות וגרפים, אלא אנליסטים מבוזרים שבכל רגע נתון יודעים מי מנהל את הכרטיסים שמגיעים ל-soc ואיך ממשיכים את הטיפול בהם בין משמרות.
הפוקוס הוא על ניהול יעיל ויצירת אוטומציות שנותנות מענה למקרים הטיפוסיים.

מיכאל: כמה אתם מעריכים שהארגון שלכם משתפר בשנה האחרונה ? ועל פי איזה מדד וכמה זה קרוב לאופטימלי ? בהנחה שזה קשה מעניין לדון בשאלה מה מושך אותנו אחורה, מה הופך את זה לקשה, יכולות, ידע ?

הדיון נסוב סביב אילו מדדים רואים ועוקבים אחריהם לאורך זמן - החל מאחוז איתור פישינג וכלה במדדים של operations בסיסיים.
בעבר ניסיתי, כל סגירה של טיקט מחייבת דיווח מלא ויש מוצרים שהוצאנו בגלל זה והבנו שהערך המוסף שלהם לא רלוונטי וגם הבנו מה הblind spot שלנו ושיפרנו את ה security posture שלנו. סוק שלא עושה את זה חי באי ודאות.

אני מסתכל על כמה דברים: על מה לא היה לי אוטומציה ? כמה פעמים התעסקתי במשהו שהוא ידני ? מבחינתי זה תקלה שבן אדם צריך לעשות מקצה לקצה תהליך. כל event שלא היה לא תהליך אוטומטי אפילו חלקי והדבר השני אם יש, כמה זמן אתה משקיע בחלק הידני, והמטרה כל הזמן לצמצם בחלק הידני. זה קשה אבל גם למכונה יש גבול כמה היא יכולה לעשות ואין מה לעשות לפעמים connecting the dots זה לא כזה טריוויאלי.
החלק השלישי, מה הן המערכות מרעישות לי יותר, האם יש מערכת שאני צריך לטייב את הרעש שלה האם יש מערכות שנעלמו לי מן הראדר ולא עשו כלום.
אנחנו בתוכניות של להפעיל צוות red team שהוא in house ונפרד לחלוטין שהמטרה שלו זה לשבור. כל הזמן לתקוף.

שאלה של אחד המשתתפים: מה יותר מדאיג אתכם, הרעש שאתם מקבלים מהמערכות או הבליינדספוט? התשובה היא בין רגל שבורה ליד שבורה?
תלוי, זה מאוד פשוט, זה סקילסט שונים, ברגע שיש את הסיגנל, אם יש לך את הסקילסט לעשות אופטימיזציה ואוטומציה אבל מצד שני אני מאוד מפחד מהדברים שלא ממופים. אני לדוגמא עובד עם הסוק שלנו ואחד המטריקות שאני מסתכל מה הכיסוי. אז לקחנו את Mitre ATT&CK והתחלנו לכסות אותו. בואו ניקח use cases שאכפת לנו מהם. נתרגם אותם לאזורים הרלוונטיים ועל זה נגיד על מה יש כיסוי ומה אין ולפי זה נראה מה controls רלוונטיים.
זה סקילטסט אחד, יש לי 7 מתוך 10 במיטרה שמתאים לuc שמדאיג אותי והמטרה שלי זה להגיע ל 9 מתוך 10. ולא כולם מדורגים באותו עומק והאיכות של הסיגנל לא שווה בין דברים ואולי צריך קורלציות. מבחינת רמת הדאגה, אני הרבה יותר מודאג, מהכיסוי, כי ברגע שאני מגיע לסיגנל שנכנס אז בין כלים אוטומטיים לבין אנליסטים, המדידה של הסוק היא לפי עבודה ידנית. תראו לי שאתם עושים אורקסטרציה כדי לפנות לכם זמן לעבוד על דברים שבאמת יותר מעניינים.

עולה השאלה - אם חברה לא נמצאת ברמת הבשלות הזו - לאיזה כיוון היא צריכה ללכת על מנת להגיע לשם?
אתה צריך להבין שמה חשוב זה המשקולות, בסופו של דבר זה risk assessment.
הצד השני החזק יותר להגיד במה אני לא מתעסק, זה לא משהו שאנחנו מתעסקים בו ולא מדאיג אותנו.
ואת ההחלטה הזאת אתה עושה על בסיס ניתוח של הדברים שאתה כן עושה.

באזורים האלו יש הרבה כוח מול מנהלים אחרים ושמה נכנס העניין של maturity - כשאתה עולה מהרמה הטקטית של x איוונטים למספר incidents. הרבה יותר מעניין אותי מה היה ה - coverage או שזה ירידה בסיגנל הרע שנבעה מאופטימיזציה.
ברמת המוצרים כל אחד חושב שהוא הדבר העיקרי, כי זה סתם שם בדילמה איך אני אומרת למוצר x או לפיד y שלא אכפת לי ממנו.

הדיון המשיך לעסוק באיזה frameworks משתמשים בנוסף למיפוי ודיווח על סקיוריטי. הועלו מספר דוגמאות. נקודה שעלתה תוך כדי היא היכולת ליצור סטנדרטיזציה, בלי קשר לאיזה framework ספציפי יותר או פחות טוב. הפיירמורקים עוזרים להבין מה הbilnd spot.

עלתה נקודה בנוגע לניטור ה-soc ומדידת ה-coverage שלו - וניתנה דוגמה ל-mssp שהראה שיש כיסוי למקור מידע מסויים, אבל בבדיקה מעמיקה יותר ראו שהמקור אמנם מחובר, אבל לא מתבצע ניטור ללוגים החשובים שלו, כך שלכאורה היה כיסוי, אבל בפועל לא היה ניטור על הפעולות שחשובות לארגון.

באחת מהישיבות board, שאלו אותי, כמה זה עלה ? ואז אתה שואל את הבורד, כמה יעלה לך שהביזנס לא יעבוד יום אחד ? the cost of doing bussiness ?צריך לשלוח חזרה את השאלה לבורד. מה מפחיד אותך? שאני לא יכול לעשות את העבודה? כמה זה יעלה לך שהעסק לא יעבוד עכשיו.

נושא 3 - DevSecOps

הגבולות בין it ל operation development השתבשו לחלוטין. בשנות ה-2000 ה-sdlc היה מאוד משמעותי כחלק מהתהליך.
היום בגלל ה- devops ובגלל צורת הפעולה של ארגוני פיתוח, הוא פחות רלוונטי ולכן נכנס הנושא של dev sec ops.
כל העניין של security ו - development הוא השתנה/בעייתי
איפה נמצאת האחריות ?
הטענה היא שכמות הטעויות שנעשו היא דווקא גדולה, כי development פתאום צריך לעשות דברים של operations והפוך. יש learning curve בעיקר למי שעובר את ה transition מארגון שהוא יותר traditional ל devops ועם זה יש יותר טעויות.

נקודות לדיון:
האם dev sec ops קיים ? האם יש כזה תפקיד, האם יש כזאת פונקציה, מי התפקידים או האנשים ברמת טייטלים הלוקחים חלק בתהליך שנקרא security ב devops
האם זה ה engineering ? למי הם מדווחים ? האם זה הchampions ?
בסופו של דבר ה accountability היא על האנשים שעושים deployment והם לא מדווחים security. הום application owner הם חתומים על האפליקציה.
מה האיכות של ה - ops ?
פעם היו אנשים, שהיו מקנפגים bgp networking והיו עושים שרתים, אופטימיזציות, מקפמלים מודולים לקרנל והיום זה ה developers שאין להם את המומחיות הזאת.
איפה אנחנו מאבדים את ה- fidelity ? בסופו של דבר איך מודדים את ה application security ?
איך נראה sdlc מודרני ?

דיון:
האם dev sec ops קיים ? כן. קודם כל זה תחום, יש בו מנעד רחב של עשייה, מי עושה את זה ? אני חוזר לשאלה הקודמת . האם יש את האנשים האם יש את הידע לעבוד עם האנשים. ואם אין לך את הידע אז מה אתה עושה ? העולם השתנה.

בארגון מה שחשוב זה awareness ואתה חייב להסתמך על זה.

אני מדבר על כלים ואני מתכוון לידע. מודעות זה נהדר אבל אנחנו מביאים ידע. אנחנו משתלבים בתהליכי הכשרה של מפתחים.

אני חושב שבפרטיקה, לא יעזור כל awareness education. בסוף מה שעובד זה שאתה משתלב ב pipeline. מה שכן צריך לעשות זה לדרג מה רמת risk לכל service וזה האחריות שלהם. אתה צריך להגיד להם מה הrisk של מה שהם עשו ולהגיד לא management בשביל לתת להם בראש.זה ה-scale up.

רון: באותם כלים אנחנו משתמשים בשביל להחליט מה עובר בpipeline. בעבודה הקודמת היה לנו weekly עם כל ה service owner שהם צריכים להציג מתי הם עשו pt, מתי הם עשו security static code analysis וכו׳.

מה המטריקות, מה הן ה - checkpoints שלך ? צריך מראש את התשתית הזאת בשביל להגיד שיש את הדברים האילו. דבר נוסף זה הסקיל, אני מפתח, עשיתי פליי, נשבר לי הבילד. כמפתח קל לי להבין איך אני מתקן את הבעיה, אבל אם נשבר בגלל security איך אני מלמד או נותן את הכלים של : זה נשבר כי… אצלנו משתמשים בספרייה x. מאיפה אתה מקבל את המדדים ?

משתתף חולק דוגמה מאצלנו, הבאנו איש security qa שהוא בונה מלא ספריות בדיקות למפתחים. מי שמשלם עליו זה qa אבל גייסנו אותו אלינו. הוא מנוהל מקצה לקצה על ידי האבטחה. כמו שיש חברה שבונים טסטים לצוותים הרגילים, אז צריך כזה גם לסקריוירטי.
גם אנשי qa אין יותר, זה התפזר לכל המקום.

לדעת משתתף נוסף המטמורפוזה שעבר הqa, ה security יעברו עוד עשר שנים. ciso יהיה יזם בחברה שכולם יעשו בה את החלק שלהם. כמו שאין יותר איש qa שעושה את העבודה הידני, והכל אוטומטי ויש מדדים לכל דבר. הסיסו יעשה אורקסטרציה ובעיקר יהיה advisory board, יהיה יזם בארגון. scrum master של עולם security.
המשתתף יכל לספר לכם מה קורה בארגון שמתעסק עם devops… בארגון שלא היה security עד עכשיו.
אני שיניתי את הטקסט מזה שצריך approval אמרתי שאני אתן ייעוץ, עצה.
אני לא מאשר, אני לא שער, אני עושה כמיטב יכולתי לעזור לכם אני מעלה לכם את המודעות.

משתתף נוסף: מה שעשינו כחובה, באפיק חדש שנפתח בג׳ירה, האם אתה צריך security architect. אם אתה עונה על אחת מהשאלות , כן. זה קופץ בsecurity ואז אנחנו יודעים שאנחנו צריכים לעשות review.
הבעיה שאנחנו מתמודדים איתה עכשיו, איך אנחנו בודקים שהוא עשה את זה?

הכל נדחף חזרה לפיתוח, אתה מצפה שהוא יעשה research משלו שהוא יעשה את התהליך בעצמו וזה חוזר לשלב החינוך שצריך להיות את הכלים מראש לדעת לאפנן את הצרכים של security.
הפסקנו לדבר ולהשתמש במושג application security ואנחנו מדברים code quality ואדז מגיע הקטע של הבן אדם אתה לא מדבר עם המפתח על security אלא על האיכות של הקוד שלו בנוסף נתתי לו את הכלים, את הדשבורד והמטריקות שהוא צריך.

זה חייב להיות בשפה שלו.

החלק של ה security ב-devops, הוא כורך בתוכו אחריותיות שנתפס הרבה יותר מאיכות. ולכן גם מפתחים ואנשי אופרציה מעדיפים לא להתעסק עם זה. אנחנו בדור המעבר, אנחנו בשלב שהאנשים היום התרגלו שיש דבר כזה סייבר, עוד כמה שנים זה יהיה הזוי שיהיו שירותים כמו 2fa.
כמו שפעם לא מפתחים לא היו נוגעים בפרודקשיין אבל היום הם נוגעים בפרודקשיין.
חלק מהחינוך שלנו זה להסביר לאנשים שזאת העבודה שלהם, זאת העבודה שלך, אני יעזור לך אבל אתה צריך לעשות את זה.

משתתף חולק דוגמה: הצוות שלי עוזר למפתחים בכל מיני תהליכים שהם עושים, אבל יש ביום יום דברים שהם חייבים להבין, אל תפתח bucket החוצה, ברור שיש אוטומציה שמתריעה לי, אני יודע להגיד את זה, אבל זה גם באחריות שלהם לא לעשות את זה.
נגיד ויש באקט שנהיה פאבליק, יש אלרט, מי מסתכל על זה? האם זה לא הגיוני שהאחריות היא של צוות ה devops ? האם זה נכון ש security מסתכל על זה.
זה מתחבר לדיון השני, עודף התראות וכמה אתה מתעסק בזה.
זה shared responsibility, אני בונה תהליך כזה ב slack, שהם חייבים להגיב.
זה אותו דבר כמו הרשאות, מי שלא צרח את הrole שלו 90 יום…
זה מאוד מעניין, זה נכון שאנחנו דור מעבר, אנחנו לומדים לעבוד עם הדבר הזה, זה יצור חדש זה לא היה קיים..

נושא 4 - non technical risk management

מציג תחום הבעיה - ניר פרי מ-CyberWrite

ניר: אנחנו רוצים לדבר על quantification של financial cyber risk. המובילים העסקיים רוצים להבין בדולרים מה הנזק. יש איזה מחקר שמשתמשים בו בעולם שלנו, יש הרבה סיסואים following the breach.
מעניין אותנו לשמוע מה נקודת המבט שלהם,
האם הסיסו צריך לדחוף למטריקות של מה הנזק ?
איך מצדיקים roi של דבר כזה או שזה פשוט משהו שזה חלק מהתוכנית security הכללית
האם זה משהו שעושים חד פעמי או שוטף ?
נקודה יותר טכנית - על בסיס מה עושים קלסיפיקציה של הנזקים ?

דיון:
אני חושבת שגם אם אתה סיסו של חברה קטנה, אתה אחראי על risk management אתה צריך לנהל צמצום נזקים ולכן נדרשת ממך accountability, על בסיס מה מודדים את הciso. זה אחת המטריקות שצריך לכלול במארג שנקרא סיסו ותפקידו.

מבחינת risk זה מחולק ל pii breach - זה קל לעשות את זה כי יש price tag. היום יודעים בדיוק מה המספר. ואז השיקולים האחרים הרבה יותר ממוקדים. אפשר לשים את המספרים על השולחן. לפני gdpr היה מאוד קשה, היום legal באו ושמו את המספר על השולחן.

נראה לי איפה שיש רגולציה מעורבת באמת יותר קל להבין את ה$$$. אני לא מכיר הרבה חברות שיש להם חישוב מדויק ומבוסס data driven.
באותה נשימה זה די good enough.

ניר: אם הבורד היה מגדיר שזה מה שאתה צריך לעשות זה היה משנה לך מאוד.

היום סיסו לא צריך להילחם להוכיח שיש איום.
זה מצוין כי זה נותן איזשהו עוגן. זה קשור לנקודה השניה של ה roi.
גם אין פונקציה של chief risk officer.

הנקודה החשובה היא דרייבר שצריך להצמיד אחרים לפרקטיקה הכללית הזאת של ריסק לארגון שכולל כמה אלמנטים: סייבר, סיילס, אופריישין ומרקטינג ואיך זה מנוהל כתרחיש.
כי data breach זה לא אירוע סייבר זה אירוע ביזנס. הנזק היחיד הוא לא נזק סייבר.מי שלא שורד זה בגלל בעיית מוניטין. המחיר של המניה לא רק חוזר אלא עולה. תשקיע.

סקר סיכונים הוא מאוד מאוד רחב. יש סעיפים שמצאתי שהם בעיה של החברה לגייס עובדים.
השאלה שלי עד כמה מערכת אוטומטית יכולה לשקף את המציאות שלי בלי להיות משועבד למערכת כדי להסביר לה מי אני ומה אני כל הזמן וכל הזמן היא צריכה להבין ולנתח מחדש.

אצלנו אין בעיה להצדקה של הוצאות security. אבל יש ארגונים שיש להם את הבעיה הזאת, ואין לי ספק שיש ארגונים שהכלי הזה הוא מאוד חזק. אבל הכימות חייב להיות מדויק.

האם זה אנחנו צריכים להוביל את זה? או שכל אחד נותן את האינפוט שלו לגוף שמתכלל את הריסק.

ניר: פגישה revenue היא פגיעה במוניטין.

אני מסכים שזה קשה אבל אפשרי. זה שאתה מביא איתך חלק מה risk לא אומר שאתה תעשה את מיטיגציה.

זה נשמע שאני מפשט את האירוע אבל זה עולם מאוד מורכב, לפני שאני עולה risk assessment עם ההנהלה, אני חושב מאוד לפני מה שאני עושה. וזה נורא קשה. אולי המערכות האלו יכולות לייצר דיאלוג. לייצר קליברציה. זה מעגן לך את זה לקונטסט מסוים. בשורה התחתונה צריך לפשט את זה למספר.

אבל זה התהליך של זה, כמה מזה התהליך מצריך ממני לחיות את הדבר הזה. וכמה אני הוא זה שצריך להוביל את זה ברמת הארגון.

עולה שאלה בדיון: למי האינטרס להביא את הדולר, מי הowner של מערכת מהסוג הזה, למי האינטרס הכי חזק.

ניר: כאשר אתם אומרים שיש gdpr וזה עזר מאוד לקידום הביזנס. והנה זאת דוגמא חיה למה זה כל כך חשוב. זאת תבונה מאוד מעניינת.

השאלה גם מה מניע את תהליך סקר הסיכונים. ברוב החברות זה קומפליינס. המנוע המקורי לעשות סקר סיכונים. זה מגיע משם. ואז השאלה איך הארגון מתייחס לדבר הזה, זה לא מספרים, זה בני אדם, האם הם עושים את זה רק בשביל קומפליינס, זה מאוד אינדיבידואלי חשוב להבין מה הרציונל מאחורי זה.

משתתף: אני לא יכול לספר לעצמי מה הסיכונים של עצמי, חבל בעיני שה audit היא מאוד ברמה השטחית. הייתי שמח אם היה review עמוק.

ניר: אני חושב שהשאלה המעניינת היא האם באמת זה יעזור לכם לקדם את האינטרסים שלכם ?

גם אם נעשה ריאליזציה זה מאוד יעזור לנו. אני צריך לבוא עם המדע המדויק של המספר הזה.

היכולת לעמוד מאחורי המספרים האלו היא מאוד חשובה. אני לא המקצוען.

מי ה industry ? זה מאוד חשוב.

ניר: אנשים אומרים בוא תגיד לי בדיוק איך הגעת למספר, זה מאוד לא פשוט.
אתה צריך להגביל עד איזה רמה אתה נותן את השקיפות. השימוש העיקרי זה גם מול הביטוח וגם כלי עבודה לאופרציה, איך אני עושה תעדוף, למה אני משקיע יותר ב x.
כן חשוב שהמערכת תשקף את controls.

הרעיון הכללי שהחישוב של המערכות האלו שאנחנו מסתכלים על כמה דברים, פעם אחת אנחנו מסתכלים על חומרת סיכון ופעם שניה ה - probability, שני הדברים האילו מייצרים את רמת הסיכון.
אנחנו רוצים לתת את האפשרות ליצור סימולציה, תהיה לך את היכולת לקבל את המספרים ופעם שניה ושלישית, זה הסיכוי שלך זה מתבסס על ההסתברויות אבל שמתי איש שיוריד את הסיכון אז המיטיגציה גם משפיעה על הסיכון.