Information Security Magazine | מגזין אבטחת מידע וניהול סיכונים

ISSA
Information Systems Security Association

GlobalSec

מרץ-אפריל 2018

הצפנה וטוקניזציה
למימוש דרישות GDPR

מפות תקיפה עולמיות - IN

מה למדתי מעבודתי ב-SOC?

קרמפוס | לגרום לשטן לבכות



CYBERMAN | מדור קומיקס חדש!



קבוצת טיטנס סקיוריטי פיתחה את

המסלול המוביל בעולם אבטחת המידע והסייבר

CYBER SECURITY & INCIDENT MANAGEMENT

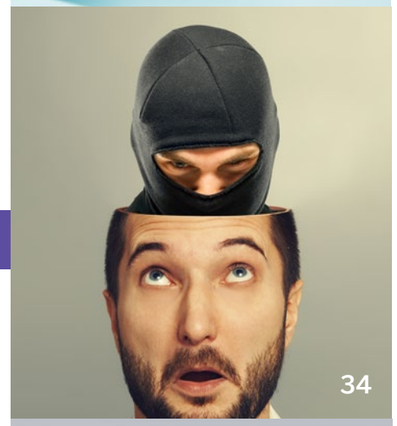
SPECIAL BOOTCAMP PREPARATION

מסלול ייחודי ובלעדי המכשיר את הבוגרים בהתמודדות יעילה עם עולם הסייבר. בוגרי הקורס ירכשו את הידע ויקבלו את הכלים בהתמודדות עם אירועי סייבר שנים. במסגרת הקורס הבוגרים ילמדו מתודולוגיות לזיהוי, טיפול וניהול אירועי אבטחת מידע.
אין מנהל אבטחת מידע לא מוצלח, יש מנהל אבטחת מידע לא מודרך!

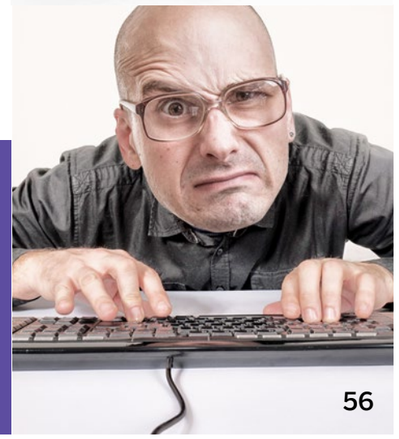
למה כדאי ללמוד אצלנו?

- הצלחה בטוחה למעלה מ-98% הצלחה בבחינות הגמר
- מיטב המרצים בתעשייה הישראלית והבינלאומית
- תרגול מעשי רב ומגוון בנושאים העכשוויים
- Networking עם מיטב הבכירים במשק הישראלי
- חברות שנתית באיגוד העולמי לאבטחת מידע ISSA ובאיגוד הישראלי
- מלגות והטבות ייחודיות לחיילים משוחררים וסטודנטים
- ערכות לימוד ייחודיות ובלעדיות


18


34


49


56

והדבר הכי חשוב, היות ואנו בטוחים בהצלחה שלנו, אנו מציעים לכלל התלמידים הטבות נוספות:

לא עברת את הבחינה?
קבל קורס חוזר ב-50%
(ללא אותיות קטנות)

עברת את הבחינה?
קבל זיכוי של עלות הבחינה,
לניצול בקורס הבא במכללת Titans security

למידע נוסף וקביעת פגישת ייעוץ:
טלפון: 077-5150340 | info@titans2.com

TSA Titans Security Academy
TSG Titans Security Group

תוכן עניינים

4 **הנדסה חברתית**
מה בעצם גורם להנדסה חברתית להצליח?

6 **עיקרון הכאוס ומלחמתו באיומי הסייבר**

מדור סיקור אירועי סייבר

10 **סוכנויות ממשל מקומיות בקונטיקט נפגעו מנוזקת כופר**

11 **אטלנטה נפלה קורבן למתקפות נוזקת כופר**

מדור תקינה ורגולציה

12 **הכה את המומחה**
ראיון עם אבי רושט

13 **הצפנה וטוקניזציה**
למימוש דרישות GDPR

מדור עמידות סייבר

16 **בקרוב שמאי סייבר?**

17 **הכירו את הסייבר רסיליינס**

מדור ה-HR

18 **5 סיבות לאיבוד הכשרונות בתחום אבטחת המידע**

22 **CISM או CISSP?**
מה ההבדלים ביניהם ולמי זה מתאים?

מדור טכנולוגיה בפוקוס

24 **עננים מאובטחים**

26 **הכירו את ה-ChatOps**

30 **ללא אכיפה אין אבטחה**

מדור יומנו של CISO

32 **תפקיד ה-CISO בעידן הסייבר**

34 **תפקיד ה-CISO במניעת אירועי סייבר**

ניהול ותגובה לאירועי סייבר

38 **מפות תקיפה עולמיות - IN**

40 **אסטרטגיות לניהול והפעלת SOC**

מדור ניהול סיכונים

42 **תקיפה על שרשרת האספקה**
למה זה צריך להדאיג אותנו?

מדור סייבר

46 **מה למדתי מעבודתי ב-SOC?**

49 **כיצד לאבטח את ה-IoT?**

מדור ספרים מומלצים

50 **Investigating the Cyber Breach**

51 **Practical Cyber**

מדור עולמו של האקר

52 **10 שלבים לביצוע מבדק חוסן מוצלח**

מדור חדשות סייבר

55 **הכירו את ה-Cloud Act**

מסיפורי הציד של קרמפוס

56 **לגרום לשטן לבכות**

קומיקס

58 **CyberMan**

בכל גיליון תקבלו חשיפה טכנולוגית על פתרונות אבטחת מידע שונים. אין אנו משמשים כגורם ממליץ, או ממליצים על מוצר כזה או אחר. מטרת הכתבות היא חשיפה טכנולוגית בלבד. כמו כן, כל הכתבות בגיליון מביאות את חוות דעתם של הכותבים, ואין זה מביע את כוונת האיגוד.

האיגוד אינו אחראי לתוכן המודעות. כל הזכויות שמורות. אין להעתיק רשימות וחלקים בלא היתר.

עורך ראשי: דני אברמוביץ
סגן עורך: יניב מילחוביץ
המערכת: TS-MEDIA
דוא"ל: info@titans2.com

GlobalSec

הנדסה חברתית



1x1

מאת: **גיא דגן**, שותף בקונסיינטה

אז מה בעצם גורם להנדסה חברתית להצליח? מדוע נחשבת הנדסה חברתית לאחת הדרכים האפקטיביות ביותר לחדור לארגונים?

ובכן אם נבחן את ההגדרה המילונית בויקיפדיה שהנדסה חברתית הנה מושג שמשמעותו ניצול של תכונות פסיכולוגיות של האדם, אשר עשויות להביא אותו לציית לבקשותיו של הפורץ. שיטה זו מאפשרת לעקוף את כל טכנולוגיות מנגנוני האבטחה (כגון אנטי וירוס, חומת אש וכו'), והיא מתבססת על העובדה שכל מערכות המידע נועדו לספק שירותים למשתמשים כלשהם, ולאותם המשתמשים יש אמצעים לגשת אל המידע שהפורץ רוצה להשיג. לדוגמה, באמצעות הנדסה חברתית, הפורץ יכול לשכנע את המשתמש לספק לו מידע רגיש כגון שמות משתמשים וסיסמאות, או לבצע עבורו פעולות כגון הרצת תוכנה לבקשתו. ואם נרצה לפשט את ההגדרה, אפשר לדעתי להגדיר הנדסה חברתית כניצול האופי שלנו נגדנו, אך הגדרה זו אינה מספקת מענה לשאלה...

וקטורי התקיפה בהנדסה חברתית ידועים ובתוכם אפשר למצוא את הבאים: Phishing, Spear-Phishing, Vishing (Voice-Phishing), Smishing (SMS-Phishing וכמובן את נושא ההתחזות והחדירה הפיזית למקומות. בנוסף קיימות עוד די הרבה דרכים בהן תוקף יכול להשתמש על מנת להוציא מידע ו/או לחדור לארגון, כגון Shoulder surfing, Tail gating, Dumpster diving ועוד רבות אחרות.

בנוסף, תפקיד המהנדס או ההאקר החברתי הפך להיות מקצוע לכל דבר אשר מצריך שימת לב לפרטים, כישורי משחק וביטחון עצמי מעבר לכישורי האקינג קלסיים.

אבל מה עומד מאחורי המושג הנדסה חברתית? מהו בעצם ה X Factor שגורם לתוקף מיומן להצליח לנצל את הגורם האנושי? על מנת להסביר את סוד ההצלחה בעיני, הבה נחזור אחורה בזמן לשנות ה 60 לניסויי מילגרם. סטנלי מילגרם היה פרופסור לפסיכולוגיה אשר ביצע ניסויים בפסיכולוגיה חברתית באוניברסיטת ייל. מכלול הניסויים נסב סביב המדידה של נכונות הנחקרים לציית לסמכות כנגד מצפונם. במפורסם שביניהם (2 Experiment) הסביר מילגרם למשתתפים שהם עומדים להשתתף במחקר שבוחן את היעילות של מתן עונש על למידה. התפקידים חולקו כך שהנחקר האמין שהוא קיבל את תפקיד ה "מורה" באופן אקראי, בעוד המשתתף השני, השחקן, קיבל את תפקיד ה "תלמיד". המורה הונחה על ידי החוקר הסמכותי (שחקן נוסף אשר שיחק פרופסור לפסיכולוגיה) שבכל פעם שהתלמיד מבצע טעות, קרי עונה לא נכון על שאלה, עליו לתת לו שוק חשמלי על ידי לחיצה על כפתור. נאמר לנחקר שיש להעלות את עוצמת השוק ב 15 וולט לאחר כל טעות. למעשה השחקן לא קיבל שוקים חשמליים כלל, אך הגיב כאילו ניתנה לו מכת החשמל. כאשר הגיעו לעוצמת שוק של 150 וולט, השחקן ביקש שהניסוי יסתיים, ונענה על ידי החוקר כי על הניסוי להמשיך. השחקן המשיך והפגין כאב וחוסר נוחות גדולים יותר, והביע חשש לביטחונו האישי אם מכות החשמל יימשכו. ל "מורים" שביקשו להפסיק את הניסוי הסביר החוקר כי הוא, החוקר, לוקח על עצמו אישית את כל האחריות לתוצאות הניסוי ולביטחונו ושלומו של התלמיד, וכי על הניסוי להימשך. בסדרה הראשונה של הניסויים שערך מילגרם, 65% מהמשתתפים נתנו את השוק החשמלי הגבוה ביותר, בעוצמה של 450 וולט, על אף שרבים לא הרגישו בנוח לבצע זאת. אף נבדק לא עצר לפני עוצמת שוק של 300 וולט!

אז מה בעצם קרה פה?

ובכן, מילגרם "בנה" את הסיטואציה ואת תנאי השטח כך שקבוצת הנחקרים הייתה נתונה להשפעת "החוקר" עד כדי כך שרוב הקבוצה בצעה פעולות הנוגדות למצפונם ובניגוד לרצונם. מילגרם בעצם "מסגר" את הסיטואציה, בודד את הנחקר עם החוקר בחדר אחד על מנת לנצל באופן מקסימלי את סמכותו של החוקר, השחקן שגילם את התלמיד הטועה ישב בחדר נפרד ללא קשר עין עם הנחקר, מה שיצר תחושת ריחוק, ניתוק וניכור אצל הנחקר. בכך עיגן מילגרם את תנאי השטח ואת ההקשר הפסיכולוגי על מנת לגרום לקבוצת המיקוד לבצע את הבלתי מתקבל על הדעת – לענות אחרים על ידי מתן שוק חשמלי. זוהי דוגמה מצוינת לעקרון הכי חשוב בעולם ההנדסה החברתית, עקרון ה "מסגור" (או Framing) של הסיטואציה או במילים אחרות ההקשר יותר חשוב מהתוכן (Context is more important than Content). הסוד להצלחה של שיטת ההנדסה חברתית הנה בנייה נכונה של הסיטואציה באמצעותה ההאקר החברתי מצליח להניע את קורבנו לבצע פעולות מסוימות או למסור את המידע אותו הוא מחפש. אין זה משנה באם מדובר בוקטור המייל (פישינג, ספיר פישינג), טלפון, SMS או בכל האמור להתחזות ולכניסה פיזית למרחבי הארגון – האקר חברתי טוב תמיד יבנה את הסיטואציה כך שקורבנו ירגיש בנח וירגיש שמסירת המידע ופעולותיו שייכות לו או טבעיות לחלוטין בסיטואציה מחד או שהוא חייב לבצע את הפעולה ולמסור את המידע כי אין לו ברירה מצד שני.

אם ניקח לדוגמה את וקטור הספיר פישינג, כל עבודת המחקר של ההאקר בבניית המייל אשר "תפור" למידותיו של קורבנו הנה בעצם פעולת "מסגור" שמבוצעת על ידו על מנת לגרום לקורבנו ללחוץ על הקישור או הצרופה הזדונית – מתן דגש על בניית ההקשר הנכון לקורבן – "מסגור" של פעולת הדיוג באמצעות לחיצה על הכפתורים שמניעים את קורבנו, באם זה שימוש בהפחדה באמצעות מייל "מהבוס" או "מסגור" התוכן של המייל שנשלח "מחברו הטוב" של הקורבן.

עוד דוגמה לכך הנה "מסגור" הסיטואציה על ידי האקר החברתי על מנת לגרום לקורבנו לבצע את הפעילות או למסור את המידע לרשותו של ההאקר, שיחת טלפון "ממחלקת ה IT והתמיכה" של הארגון שתגרום לקורבן למסור את סיסמתו או מחברת "הביטוח" של הקורבן על מנת להשיג ממנו פרטים אישיים חסויים.

באותה מידה עקרון ה "מסגור" בא לידי ביטוי בחדירה פיזית לחברות ולמקומות אליהם רוצה ההאקר לחדור, שהרי מי יעצור שליח עם קסדה אשר מגיע להביא חבילה לארגון? או הרמת טלפון מקדים שבו נמסר למזכירת הארגון ש "טכנאי של בזק" מגיע בתאריך מסוים ונדרש לארגן לו כניסה?

בניית הסיטואציה הנה אחת מעקרונות היסוד עליהם מושתתת ההנדסה החברתית, השיטות לכך רבות ומגוונות ואפשר למצוא בינן את בניית המחויבות (Creating commitment) - שהרי כולנו מכובדים ורוצים לעמוד במילתנו וברגע שהתוקף הצליח להוציא מאתנו מחויבות למשהו, רובנו נעמוד במילתנו וניטה להסכים להתחייבות גדולה יותר או מתן סיבה טובה – שהרי כולנו נתגייס למען Green Peace נכון? ואם יחתימו אותנו למענם ויבקשו את מספר הטלפון והמייל שלנו, לא ניתן? ככל הנראה רוב האנשים ימסרו פרטים אלו.

ההתגוננות בפני הנדסה חברתית מורכבת משלושה נדבכים:

בקרות ומערכות הגנה – מנגנוני בקרה ואכיפה, ניהול הרשאות, רוטציה במשרות, עקרון ארבע העיניים וכיו"ב.

נהלים – הגדרת תהליכי עבודה נאותים, הגדרת המותר והאסור וגבולות הגזרה בכל תהליך עסקי.

מודעות – שהרי קיים סיכוי לא קטן שהתוקף יעקוף את מערכות ההגנה ואז ההכרה של וקטורי התקיפה, תרגול לשיטות אלו ושיפור יכולות הזיהוי ובעיקר עצירת התגובה האוטומטית, "לספור עד שלוש" לפני לחיצה על קישורים או צרופות ובחינת המייל, בחינת הסיטואציה עצמה בזמן שיחת טלפון או בכל מקרה בהם אתם מתבקשים למסור את פרטיכם. בנוסף ברגע שהעובדים יבינו את הלמה גם הנכונות לעבוד על פי הנהלים תגבר. חינוך העובדים לזיהוי והתגוננות בפני שיטות ההנדסה החברתית הנה הדרך האפקטיבית והזולה ביותר לחזק את מערך ההגנה הארגוני ואת החוליה החלשה ולהקטין את הסיכוי לחדירה לארגון באמצעות הגורם האנושי.

ConSienta
Cybersecurity Awareness

עיקרון הכאוס ומלחמתו באיומי הסייבר



מאת **ארז קפלן העליון**, CTO CYBER2.0

במצבי מלחמה שונים, תמיד נראה, שפעם צד אחד מקדים את הצד השני, ופעם להיפך- הצד השני נמצא צעד אחד קדימה.

מדוע אם כן, בעולם הסייבר, עם אלפי חברות סייבר, שמעסיקות את מיטב המוחות בעולם, המצב הקבוע הוא, שהתוקפים תמיד נמצאים צעד אחד קדימה, ושהתקפה ממוקדת תמיד תחדור את כל מערכות ההגנה הקיימות?

הדבר הדיר שינה מעיני כבר תקופה ארוכה. מול כל מערכות הגנה הפרוסה בארגון, ובכל רמת אבטחת מידע; התוקפים תמיד מצליחים לחדור, לרגל, לנצל ולהרוס.

ההסבר לכאורה טרוויאלי: אין מערכת שהינה בלתי ניתנת לפריצה, לכן, תמיד ימצאו הפורצים דרך לחדור דרך כל ההגנות האירגוניות. כך היה מאז ומעולם, וכך סביר שיהיה לעד.

כתוצאה מכך, נמצאים אנשי אבטחת המידע במרדף מתמיד אחרי הפריצה הבאה, נערכים לקראת החדירה הקרובה, ומוצאים את עצמם טובעים בים של התרעות מתוך מערכות שונות, שאת כולן, ניתן בסופו של דבר, לעקוף.

התפיסה המקובלת אומרת, שכל מערכת הגנה הינה סוג של רשת מחוררת, ולכן, ככל שנוסיף שכבות של רשתות זו על גבי זו, כך נקטין משמעותית את הסיכוי, שהתקפה עתידית תחדור את השכבה הראשונה, וגם אם היא לא תיעצר בשנייה, הרי שתיעצר בשלישית או ברביעית.

היות ולכל רשת נוספת יש עלות, הרי שככל שהארגון מבוסס יותר כלכלית, הוא מקצה תקציב גדול יותר לתחום הגנת הסייבר, וכפועל יוצא, הוא מוגן יותר מפני התקפות עתידיות.

כל פתרון חדש שצץ חדשות לבקרים, בא למעשה לתת פתרון לסוג התקפה חדש, שעד כה לא נבלם באמצעות מערכות ההגנה הקיימות.

מערכות הסייבר בעולם, הן ההתקפיות והן ההגנתיות, מבוססות על מודלים ביולוגיים; במשך מיליארדי שנות חיים, ביסס הטבע מערכות הגנה יעילות ומתקדמות, שאך טבעי הוא לחקור ולחקות אותן. ואולם, גם הטבע עצמו נמצא באותו לופ אינסופי; התוקפים מוצאים פירצה, משנים את מודל התא, מפתחים עמידות או יוצרים מוטציה חדשה. והטבע, באיחור אופנתי, מאתר ופותר את הבעייה. "וירוסים" ו"אנטי וירוסים" הינם לא במקרה, מונחים השאולים מעולם הטבע.

נדמה, שהתוקפים בסייבר אף מתוחכמים יותר מהתוקפים בטבע. כל למשל, נוכל לראות מקרה בו התוקפים פורצים לארגון דרך המשתמשים שלו, באמצעות שליחת לינק או דוא"ל, עוברים את מערכות ההגנה הידועות, ומתקינים את עצמם, לכאורה באישור המשתמש (וללא ידיעתו, כמובן) תוך כדי התחזות לתוכנה מוכרת, אם זה תוסף לדפדפן, מקרו באקסל, או שדרוג של קורא PDF וכדומה. ובשלב הבא, לאחר

שהתוכנה הזדונית הצליחה לשטות בהגנה הראשונית, היא מנטרלת באופן שיטתי את כל ההגנות הקיימות, ומתפשטת ברשת האירגונית ("Lateral movement"), מצפינה קבצים, שולחת מידע החוצה, מאפשרת שליטה מרחוק או סתם ממתינה לקבלת הוראות מהשולחים שלה.

כיצד, אם כך, שוברים את המעגל האינסופי הזה?

בשלב הראשון הבנתי, שעל הפתרון להגיע מחוץ לעולם הביולוגי. עדיין לא היה ברור מאיזה עולם הוא עתיד לבוא. עיקר הקושי נבע מהעובדה, שחדשות לבקרים התפרסם מחקר חדש, שפיצח את הדרך שבה פועלים כוחות הטבע, וניסה לחקות אותן (כיצד הדבורים מתקשרות בינהן, כיצד פועלות פטריות, כיצד וירוסים וחיידקים מרמים את מנגנוני ההגנה בגוף ועוד כיו"ב), מאידך, היה ברור, שכל פתרון כזה, מבוסס מודל ביולוגי כזה או אחר, יסבול באופן מובנה מאותן בעיות.

לפני כשלוש שנים, האזנתי לתחזית מזג האויר. דיברו על כך שהוא הפכפך, ובלתי ניתן לצפייה. המונח שחזר ועלה היה "כאוס". גוגל טרנסלט מגדיר כאוס ב"תוהו ובוהו" וחוסר סדר. ואולם, "תורת הכאוס" הינו מונח מתחום המתמטיקה. הוא מונח שדווקא מבטא סדר. לא סתם סדר- אלא סדר מושלם; שתי מערכות שיתחילו מאותה נקודה, ויעברו דרך אותו מסלול- תמיד יביאו לתוצאה זהה לחלוטין. אך השינוי הקל ביותר באחת המערכות בדרך, יגרום לסטייה הולכת וגדלה שלה עם הזמן- ולתוצאה שונה לחלוטין. מערכות הכאוס הינן דינמיות, עם רגישות גבוהה מאוד לשינויים אפסיים.

חשבתי שניתן לבנות מערכת, המבוססת על אותם חוקי כאוס, אך עושה שימוש בציר מתמטי במקום ציר זמן, ואשר הסיכוי שהיא תהיה ניתנת לפריצה, גם אם כל האקרים בעולם ינסו לתקוף אותה, יהיה שקול לסיכוי שכל מומחי החיזוי והמדעים יוכלו לפצח את מערכת מזג האויר, באופן שיאפשר להם לתת תחזית מדוייקת ביותר, לכל דקה בכל יום במהלך 15 השנים הבאות.

על המערכת הזאת עבדתי מספר שנים עד לפיצוח שלה.

על בסיס זה הקמתי את Cyber 2.0, שיוצרת סוג של הגנה וירטואלית בטווח שבין המחשבים, תוך שהיא מסתמכת על איזון כאוס של התקשורת בינהן, כאשר כל ניסיון להפיל, לעקוף או לרמות את המערכת, יגרום להפרת האיזון שנוצר על ידי הכאוס בין המחשבים, ולחסימה של הקוד הזדוני.

כל המערכות הקיימות היום בעולם הסייבר מתנהלות על פי אותו עיקרון, קודם Detection ואז Prevention. דהיינו, קודם מנסים לזהות את התוכנות הזדוניות, ואז לבלום אותן או להתריע עליהן. מטבע הדברים הזיהוי אינו יכול להיות מוחלט. ואלם, Cyber 2.0 מדלגת שלב; חסימה ללא זיהוי, תוך שימוש בעקרון הכאוס.

גם בשלב החסימה אנחנו מזהים כשלים במערכות הסייבר הקיימות, שנובעות מכתוצאה מהפלת המערכת או מעקיפתה בידי התוקפים. הפלת המערכת, תפיל יחד איתה את החסימה.

מערכת Cyber 2.0 תמשיך להגן על הארגון, גם אם היא תופל לחלוטין, תיפרץ, תוסר או תעבור כל שינוי אחר.

כיצד זה יתכן? הארגון מגדיר מהן התוכנות המורשות לצאת מגבולות המחשב (מדובר על מספר עשרות תוכנות, שהותקנו כולן בידי מנהלי הרשת, וכוללות אאוטלוק, הנהלת חשבונות, אופיס וכיו"ב) ואותן נגדיר כ"תוכנות הלגיטימיות".

כל תוכנה שלא הוגדרה כלגיטימית, בין אם היא אכן לא לגיטימית, והין אם היא וירוס חדש ולא מוכר, או כל תוכנה אחרת- תוגדר אוטומטית כ"לא לגיטימית".

בניגוד לכל תוכנות הסייבר האחרות, המנסות לעצור את מה שנראה להן לא לגיטימי, מערכת Cyber 2.0 המותקנת בכל מחשב, פועלת בדרך הפוכה: אם התוכנה הוגדרה כלגיטימית- המערכת מערבלת לה את הפורט דרכו היא יוצאת. בכניסה למחשב הבא, הפורט מתערבל עירבול נוסף, שמחזיר אותו למספרו המקורי, והוא נכנס כמתוכנן למחשב התקין.

אם לעומת זאת, התוכנה המנסה לצאת לא הוגדרה כלגיטימית, הפורט ביציאה לא יעורבל, אך בכניסה למחשב הבא- הוא יעורבל, ולכן ייחסם.

מדוע המערכת כה עוצמתית? מכיוון שכל נסיון לעקוף את התוכנה או לחדור אותה, יגרום לתוכנה הזדונית לצאת בפורט המקורי שלה. ואולם, מלכתחילה מערכת Cyber 2.0 היתה אמורה לתת לה לצאת בפורט המקורי שלה, כך שהפלת המערכת או עקיפתה- לא יגרמו לכל שינוי, והתוכנה תיחסם.

גם נסיון לשנות את רשימת התוכנות הלגיטימיות נידון לכישלון, היות ומנגנון הכאוס יבלום אותו.

מה זה בעצם אומר?

ראשית- עצירה מוחלטת של כל התקפת סייבר מכל סוג ומכל מין, כולל התקפות חדשות ובלתי מוכרות. כאן נשאלת באופן טבעי השאלה, כיצד בעצם ניתן לזהות התקפות חדשות ובלתי מוכרות לחלוטין? אכן לא ניתן! אך כאמור, Cyber 2.0 חוסמת אותן, בלא שהיא אפילו נדרשת לזהות אותן.

שנית- לא עוד מרוץ בלתי פוסק של תוקף > מגן> תוקף וחוזר חלילה.

והעיקר- אין יותר צורך בשכבות רבות של הגנה, אין צורך ברדיפה אחר התראות וניתוחן, ויש בעיקר שקט נפשי.

ולסיום, השיטה יעילה לא רק נגד כל סוגי ההתקפות בארגונים. היא ניתנת ליישום גם במחשבים בבית, וגם בכל תחום ה IOT, לרבות תחום המכוניות האוטונומיות.



קבוצת טיטנס סקיוריטי פיתחה את

המסלול המוביל בעולם כהכנה לבחינת ההסמכה של CISSP

CISSP SEMINAR

SPECIAL BOOTCAMP PREPARATION

זהו המסלול היחיד שכולל הכנה מלאה לבחינות ההסמכה בפורמט החדש (100% הצלחה בבחינות האחרונות) כי אין מנהל אבטחת מידע לא מוצלח, יש מנהל אבטחת מידע לא מודרך!

למה כדאי ללמוד אצלנו?

- הצלחה בטוחה למעלה מ-98% הצלחה בבחינות הגמר
- מיטב המרצים בתעשייה הישראלית והבינלאומית
- תרגול מעשי רב ומגוון בנושאים העכשוויים
- Networking עם מיטב הבכירים במשק הישראלי
- חברות שנתית באיגוד העולמי לאבטחת מידע ISSA ובאיגוד הישראלי
- מלגות והטבות ייחודיות לחיילים משוחררים וסטודנטים
- ערכות לימוד ייחודיות ובלעדיות

והדבר הכי חשוב, היות ואנו בטוחים בהצלחה שלנו, אנו מציעים לכלל התלמידים הטבות נוספות:

לא עברת את הבחינה?
קבל קורס חוזר ב-50%
(ללא אותיות קטנות)

עברת את הבחינה?
קבל זיכוי של עלות הבחינה,
לניצול בקורס הבא במכללת Titans security

למידע נוסף וקביעת פגישת ייעוץ:
טלפון: 077-5150340 | info@titans2.com

TSA Titans Security Academy

TSG Titans Security Group

סוכנויות ממשל מקומיות בקונטיקט נפגעו מנוזקת כופר

נוזקת הכופר הידועה לשמצה בשם WannaCry מצאה את דרכה אל כ-160 מחשבים ב-11 סוכנויות ממשלתיות מקומיות בקונטיקט, שבארה"ב.

ביום שישי אחר הצהריים, הנהלות הארגון ביחד עם צוותי התגובה וצוותי ה-IT הוזקו למקום, לאחר שמערכות הניטור גילו את ההידבקות בנוזקה בחלק מהמחשבים. צוותי התגובה וה-IT עבדו במהלך כל הסוף שבוע, והצליחו לבודד את התפשטות הנוזקה לשאר המחשבים והמערכות ברשת.

מרבית המחשבים לא נדבקו בשל תהליך נאות של ניהול טלאים והקחת מערכות ההפעלה, כולל התקנת אנטי-וירוס במחשבי הקצה. "בד"כ אנחנו עושים עבודה טובה מאוד בסגירת הפרצות מבוא מועד, אמר מארק ריימונד, מנמ"ר הממשלה. בארגון יש למעלה מ-30,000 תחנות עבודה, והעובדה שהנוזקה הצליחה להדביק חלק מהמחשבים, מעיד על כך שחלק מהמחשבים נפלו בין הכסאות, ולא עודכנו והוקשחו כפי שצריך", עוד הוסיף מארק.

האירוע עדיין תחת חקירה של גופי הביטחון וצוותי התגובה במשרד. כל מערך המחשוב במשרדי הממשלה נמצאים כעת בתהליך מדוקדק של התאוששות מהאירוע, שכולל בין היתר לנסות לאתר את כל ההתקנים שנבדקו בנוזקה, לנסות לבודד אותם, למצוא את מקור הבעיה, ולהתקין אותם מחדש, כולל הקשחה וניהול טלאים באופן מלא.

צוותי התחקור הדיגיטלי בוחנים את מערכות הניטור ואת הלוגים של כלל המערכות שהיו מעורבות בתקרית, לצורך הפקת לקחים. "עד כה לא היה לנו אירוע כזה", אמר ריימונד.

נוזקת ה-WannaCry הופיעה לראשונה במאי 2017, ומאז הצליחה להדביק מאות אלפי מחשבים ברחבי העולם. הנוזקה מנצלת פגיעות במערכת ההפעלה של Windows, שקיים לה כבר עדכון (טלאי).

ברגע שהנוזקה מצליחה להדביק את המחשב, היא מצפינה את כלל הקבצים במחשב ומבקשת כופר מהקורבן, בד"כ בביטקוין, על מנת לקבל חזרה את מפתח ההצפנה.

עד כה, לא נמסר על איבוד מידע רגיש כתוצאה מהתקרית, אך האירוע עדיין תחת חקירה פדרלית.

אבל קונטיקט אינה המדינה היחידה שספגה מתקפות סייבר מוצלחות. משרד התחבורה בקולורדו וגם העיר Allentown שספנסילבניה סבלו ממתקפות סייבר גדולות במהלך החודש האחרון. בעוד שמשרד התחבורה בקולורדו הצליח לשזחר את המידע האבוד (שהוצפן ע"י הנוזקה) באמצעות גיבויים מהאתר המרוחק, המתקפה שאירעה בעיר Allentown שבפנסילבניה עלולה לעלות לעירייה למעלה ממיליון דולר, עפ"י הדובר של העיריה.



בעקבות מתקפת סייבר שהצליחה להדביק מחשבים בנוזקת כופר, משרדי הסוכנות הממשל המקומית באטלנטה עובדת בשיתוף עם ה-FBI, המחלקה לבטחון המולדת, וצוותי תגובה של חברת Microsoft ו-Cisco כדי לקבוע את היקף המתקפה ולנסות לנקות את המחשבים מנוזקת הופר.

נראה שהמתקפה השפיעה על מספר מערכות פנימיות, שחלקן פתוחות לציבור, ומאפשרות ביצוע תשלומים כגון אגרות וגישה למידע הקשור לבתי המשפט, אמרו גורמים רשמיים מהעירייה.

עפ"י ההודעה שהופיעה בנוזקת הכופר דרשה, התוקפים דרשו 51,000 דולר או 6,800 דולר כדי לפתוח את ההצפנה על כל מחשב, נמסר ע"י גורמים רשמיים מהעירייה.

במסיבת עיתונאים, אמר ריצ'ארד קוקס, מנהל התפעול (COO) החדש של העירייה, כי מספר מחלקות בעירייה הושפעו, אך לא אלו הקשורות לביטחון הציבור, למים או למשכורות.

ראש העיר קיישה בוטומס, אמרה כי העירייה טרם קבעה האם נתוני העובדים נפגעו, והיא מייעצת לעובדים להיות זהירים במיוחד, ולפקח באופן יזום על חשבונות הבנק האישיים שלהם ולשים לב לכל חריגה בחשבון או בפעילות כרטיסי האשראי. כמו כן, כל מי ששילם חשבונות לעיר אטלנטה או קיבל תשלומים, כמו גמלאים, צריך להיות ערני, בזמן שהחקירה עדיין נמשכת, היא אמרה.

אטלנטה נפלה קורבן למתקפות נוזקת כופר

לאחר שמספר סוכנויות ממשל מקומיות נפלו קורבן למתקפות נוזקת כופר מתחילת השנה, הגיעה תורה גם של מדינת אטלנטה לעלות לכותרות. עפ"י הערכות, מדובר בקמפיין מאורגן כנגד סוכנויות ממשל מקומיות ברחבי ארה"ב.

האסטרטגיה של העירייה להעביר חלק ממערכות המחשוב לענן, כחלק מהאסטרטגיה של ממשל אבטחת המידע וטכנולוגיות המידע הוכיחה את עצמה, וזה הפחית חלק מההשפעות של התקרית סייבר, אמרה דפני רקלי, המנמרית (CIO) של העיר אטלנטה. במטרה לשפר את רמת אבטחת המידע, העירייה העבירה חלק גדול מהמערכות המחשוב שלה לענן.

כאשר נשאל על הטיפול או המלצות לטיפול באירועים מסוג זה, ראקל הצביע שוב על הענן. " יש לנו אסטרטגיה למחשוב ענן, כך שאנחנו מתכוונים להעביר את כל המערכות הקריטיות שלנו לתשתית ענן, שהיא סביבה מאובטחת יותר ממה שקיים אצלנו היום".

בעוד שראקלי לא שיתפה מידע רב אודות היקף התקיפה ומהות הפגיעה (מבחינת מידע אודות הגנת הפרטיות), היא הדגישה את השקיפות בכך שהעירייה דיווחה לציבור באופן מיידי עם גילוי המתקפה, בניגוד לחברות אבות שנפלו קורבן למתקפות סייבר אך דיווחו על כך ימים או שבועות מאוחר יותר.

אומנם לא כל הרשתות של העירייה נפגעו, סוכנויות הממשל המקומי נקטו אמצעי זהירות נוספים. עובדי בעירייה הונחו לא להפעיל את המחשבים שלהם או להיכנס לתחנות העבודה שלהם במהלך הסופ"ש.

שדה התעופה של אטלנטה הורידו את הרשתות האלחוטיות בשדה, וגם חלק מהאתרי אינטרנט שלהם. מדובר הרשמי של שדה התעופה נמסר כי, אומנם שדה התעופה לא נפגע ממתקפת הסייבר שפקדה על עיריית אטלנטה, ההנהלה החליטה לנקוט בצעדי זהירות ולמזער את הסיכון לפגיעה כתוצאה מאירוע סייבר נוסף.

גם שירותי ההצלה (חיקום) והמשטרה (911) לא הושפעו מהמתקפה, דיווה מפכ"לית המשטרה אריקה שילדס. עם זאת, המשטרה, מתוך משנה זהירות, בחרה לעשות שימוש בדיווח דוחות ידני (נייר) במטרה למנוע פעילות מיותרת במערכות המחשוב במשטרה, ולמזער את ניסיונות התקיפה. "מלבד היכולת לגלוש באינטרנט, המשטרה עדיין פעילה במלואה, ללא כל השפעה מהותית", היא הוסיפה.

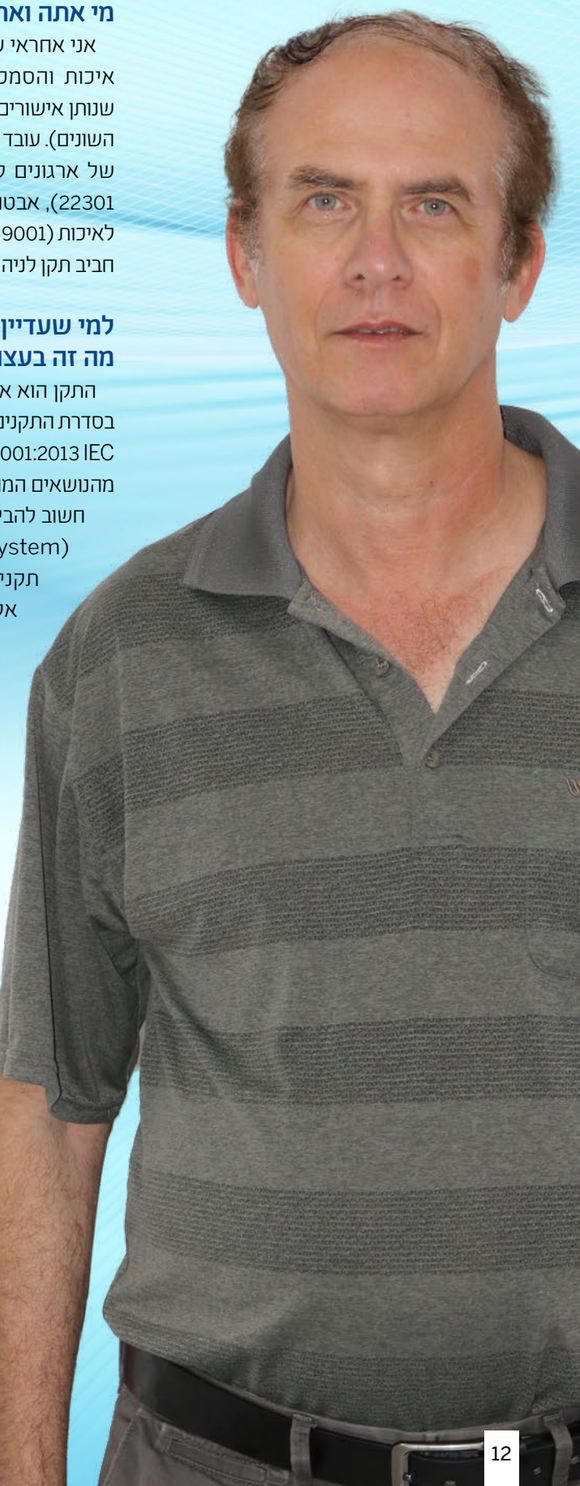
כפי שדובר עיריית אטלנטה מסר לעיתונות, לא מדובר במקרה ראשון, אלא ניכרת כאן מגמה של ניסיונות פגיעה במספר מטרות בתוך הממשל המקומי בארה"ב. מלבד עיריית אטלנטה, היו עוד גופים רבים שנפגעו מתקיפות סייבר (נוזקות WannaCry) כגון סוכנויות הממשל המקומי בקונטיקט, מחוז קארול (Carol County), משרד השריף, מחוז מונגומרי, מחוז מקלנבורג, ועוד מחוזות רבים אחרים.

מומחי אבטחה ציינו שקבוצת האקרים בשם TheDarkOverlord ניסתה למכור רשומות של מידע רגיש (PII) שנגנבו באמצעות נוזקת כופר, מלמעלה מ-100 בתי ספר וגופים עסקיים.

"זה לא שמשרדי הממשלה חשופים יותר לפגיעויות ותקיפות סייבר מאשר המגזרי הפרטי, אלא הם מהווים מטרות סקסיות יותר בעיני התוקפים", אמר סמנכ"ל עיריית אטלנטה. מערכות המידע הממשלתיות צריכות להיות נגישות לציבור הרחב, על מנת לאפשר להם לבצע תשלומים באופן מקוון או למצוא מידע שימוש עפ"י הצורך כך שזה אוטומטית הופך אותן למטרות מבוקשות יותר בעיני התוקפים. ולכן, המערכות הללו חייבות להיות מאובטחות הרבה יותר", הוא הוסיף.

הכה את המומחה

ראיון בלעדי עם מר אבי רושט, סוקר מוביל ממכון התקנים, אודות התקן הגנת הפרטיות במחשוב ענן (ISO 27018)



מי אתה ואת מי אתה מייצג?

אני אחראי על תחום אבטחת המידע באגף איכות והסמכה של מכון התקנים (האגף שנותן אישורים על עמידה בדרישות תקני ISO השונים). עובד במכון התקנים כ 12 שנה, כסוקר של ארגונים לתקן המשכיות עסקית (ISO 22301), אבטחת מידע לתקניה השונים, תקן לאיכות (ISO 9001) בחברות תוכנה IT, ואחרון חביב תקן לניהול ידע (ISO 25006).

למי שעדיין לא מכיר או לא יודע, מה זה בעצם תקן ISO 27018?

התקן הוא אחד ממדריכים שונים שפורסמו בסדרת התקנים 270xx, המתלווים לתקן /ISO IEC 27001:2013, ומהווים השלמה לתקן באחד מהנושאים המופיעים בו.

חשוב להבין שמדובר לא ה "מערכת ניהול" (Management system) כדוגמת תקני ISO 27001 או ISO 9001 אלא במדריך ליישום (Code of practice).

במה עוסק התקן ISO 27018?

הוא מהווה מדריך ליישום הגנה על מידע פרטי, הנמצא בענן ציבורי הפועל כ "מעבד מידע" (PII Processor).

למי מיועד התקן ISO 27018?

לכל ארגון הפועל כמעבד מידע פרטי (PII processor) או מפקח המידע (PII controller). יש להבהיר את מערכת היחסים, בין הגופי השונים ולהגדיר מי ה principle (מושא המידע), ה processor (מעבד המידע), וה controller (קובע חוקי ההתנהלות, גם ארגון המפעיל ספקים גם רגולטור).

מה דרישות התקן ISO 27018?

התקן בנוי משני חלקים .

הבקרות המופיעות בתקן ISO 27001, ואיך הן צריכות להיות מיושמות בהקשר של מידע פרטי, ונספח של בקרות נוספות הייחודיות לתחום זה

בנוסף קיימות דרישות המופיעות תקן ISO 29100 המהווה בסיס הגדרת של צורת הניהול של מידע פרטי.

מה ההבדל בינו לבין תקנים אחרים כמו תקנות הגנת הפרטיות או ה-GDPR?

שתי הרגולציות שהוזכרו עוסקות במידע פרטי באשר הוא ו-ISO 27018, עוסק במידע בענן ציבורי בלבד

מי נותן הסמכה ומה נדרש כדי לקבל הסמכה ISO 27018?

מכון התקנים כגוף התקינה הלאומי של ישראל אימץ את התקן בצורתו הבינלאומית, ואגף איכות והסמכה (שאני משתייך אליו) פועל להסמיך (המונח המדויק הוא "להתעיד" To certificate) ארגונים המבקשים זאת.

מה לדוגמה עוסק התקן ISO 27018?

נושאים לדוגמה: רישום לוגים של אירועים של חשיפת מידע פרטי, איסוף מידע רק לצורך מוגדר, בדיקה שמידע הנאסף הוא אמין ומדויק לפני העיבוד שלו, זכותו של מושא המידע (PII principle) לראות מה המידע שנאסף עליו (ראה מקרה פייסבוק לאחרונה).

מה נדרש לעשות כדי לעמוד בתקן ISO 27018?

מלבד הפעולות האדמיניסטרטיביות מול מכון התקנים(מידע נוסף נמצא באתר מכון התקנים וניתן אף מומלץ להיעזר ביועצים המתמחים בנושא) יש להכין סדרתי מסמכים ע"פ הנדרש בתקן (רשימה זו ניתן לקבל מסוקרי המכון - מסמי מדיניות, נהלים, ותיעוד נוסף (דוגמה מדינות בהן ה-public cloud PII processor שומר את המידע).

הצפנה וטוקניזציה למימוש דרישות GDPR



מאת **יניב מילחוביץ**, סמנכ"ל חברת הייעוץ טיטנס סקיוריטי

טוקניזציה והצפנה הן בקרות שמוזכרות לעתים קרובות כאמצעי לאבטחת המידע המועבר ברשת האינטרנט (Data in Transit) או המאוחסן במנוחה (Data at Rest). בנוסף לעמידה בדרישות מדיניות אבטחת המידע של הארגון, השימוש בטוקניזציה והצפנה מסייעים גם בהלימה לדרישות תקינה ורגולציות רבות כגון PCI-DSS, HIPAA, GLBA, ITAR וכמובן ה-GDPR.

בעוד טוקניזציה והצפנה הן טכנולוגיות אפקטיביות לטשטוש הנתונים, הן אינן זהות, ולא ניתן להשתמש באחת מהן במקום השנייה. לכל טכנולוגיה יש נקודות חוזקה וחולשות משלה, ועל בסיס אלה, הארגון צריך לבחור את השיטה המועדפת עליו לאבטחת נתונים בנסיבות שונות. במקרים מסוימים, כגון עם נתוני תשלום אלקטרוניים (נתוני כרטיסי אשראי) ניתן להשתמש בשתי השיטות עדי להבטיח את אבטחת הנתונים מקצה לקצה.



הצפנה

הצפנה היא תהליך של שימוש באלגוריתם מסוים כדי להפוך מידע שמוצג בטקסט רגיל (גלוי) לטקסט מוסתר, בפורמט לא גלוי, שנקרא טקסט מוצפן (cipher-text). לצורך הפענוח של המידע, יש צורך להשתמש באותו אלגוריתם ששימש בתהליך ההצפנה ובמפתח הצפנה (מעין קוד מתמטי).

בעידן הטכנולוגי של היום, באמצעות יכולות הצפנה מובנות של מערכות ההפעלה או של כלי הצפנה של צד שלישי, מיליוני אנשים מצפינים נתונים במחשבים שלהם כדי להגן מפני גישה (קריאה) של גורמים לא מורשים של הנתונים הרגישים במקרה שהמחשב שלהם נגנב או נאבד. כמו כן, השימוש בהצפנה הינה השיטה היעילה ביותר למנוע גישה לא מורשית לנתונים הרגישים שלנו.

ישנם שתי שיטות הצפנה עיקריות: הצפנה סימטרית והצפנה א-סימטרית.

בהצפנה סימטרית, אנו משתמשים באותו אלגוריתם ובאותו מפתח הצפנה לצורך הצפנה ופענוח של המידע שמועבר בין שני גורמים. הצפנה באמצעות מפתי סימטרי, דומה לתהליך נעילת הדלת של הבית עם מפתח אחד, שיכול להיות משוכפל לכמה דיירים, ולשמש לצורך נעילת ופתיחת הדלת.

ישנן מספר בעיות בשימוש בהצפנה סימטרית, כגון כיצד נוכל לאבטח את המפתח ולמנוע גישה למפתח מפני גורמים שאינם מורשים לכך. באם גורם עוין השיג את המפתח, הוא יוכל להשתמש בו לפענח את המידע שהוצפן. חסרון נוסף הינו תהליך הפצת המפתח. כיצד ניתן להפיץ את המפתח בצורה מאובטחת. ישנם חסרונות נוספים כגון תהליך ניהול המפתחות, אבל זה פחות רלוונטי להיבטים של אבטחת מידע, אלא יותר לנושא התפעולי.

מסיבה זו, פותחה ההצפנה הא-סימטרית. ההצפנה הא-סימטרית משתמשת בזוג מפתחות: מפתח פרטי ומפתח ציבורי, כאשר ביניהם יש קשר מתמטי, כך שאם בצענו פעולה עם אחת המפתחות, הפעולה ההפוכה צריכה להתבצע עם המפתח השני.

למשל: לצורך הצפנת מידע רגיש, השולח ישתמש במפתח הציבורי של הנמען, ובצד השני, הנמען ישתמש במפתח הפרטי שלו על מנת לפענח את המידע.

לצורך חתימה על מסר מסוים, השולח יחתום עם המפתח הפרטי שלו, ובצד השני, הנמען יאמת את התהליך באמצעות המפתח הציבורי של השולח.

עד עכשיו, אחד החסרונות המהותיים של שימוש בהצפנה בתוך יישומים, הוא כי ההצפנה לא מאפשרת שימוש בחלק מהפונקציונאליות של היישומים, כגון מיון וחיפוש.

טוקניזציה

טוקניזציה הוא תהליך של הפיכת נתונים משמעותיים (כגון מספר חשבון בנק, מספר כרטיסי אשראי, מספר תעודת זהות וכדומה) לתוך מחזורת אקראית של תווים הנקראים אסימון (token) שאין לו ערך משמעותי אם הוא מגיע לידיים הלא נכונות. האסימונים הללו

משמשים כנקודת התייחסות לנתונים המקוריים, אך לא ניתן להשתמש בהם כדי לנחש ערכים אלו. הסיבה לכך היא, שלא כמו בהצפנה, הטוקניזציה אינה משתמשת בתהליך מתמטי כדי להפוך את המידע הרגיש לתוך האסימון. אין מפתח הצפנה, או אלגוריתם, שניתן להשתמש בהם כדי להפיק את הנתונים המקורים עבור האסימון. במקום זאת, הטוקניזציה משתמשת במסדי נתונים, הנקרא כספת אסימונים (token vault), שמאחסנת את הקשר בין הערך הרגיש לבין האסימון. הנתונים האמיתיים בכספת מאובטחים, בדרך כלל באמצעות הצפנה, בקרת גישה מוגבלת וניטור של כלל הגישה והשימוש בטבלאות הללו, מה שמונע את ממזער באופן משמעותי את הסיכון לגישה למידע הרגיש.

ניתן להשתמש בערך העסימון ביישומים שונים כתחליף לנתונים האמיתיים. אם הנתונים האמיתיים צריכים להיות מאוחזרים – לדגומה, במקרה של תשלום חוזר בכרטיס האשראי של הצרכן – האסימון נשלח לכספת והמפתח קישור משמש כדי להביא את הערך האמיתי לשימוש בתהליך ההרשאה. מבחינת משתמש הקצה, פעולה זו מבוצעת בצורה שקופה, באמצעות הדפדפן או היישום. סביר להניח שהמשתמשים אינם מודעים לכך שהנתונים מאוחסנים בענן בפורמט אחר.

היתרון הטמון בשימוש באסימונים הוא שאין קשר מתמטי לנתונים האמיתיים שהם מייצדים. אם הפ נפרצו, אין להם משמעות. אין מפתח שיכול להפוך אותם בחזרה את ערכי הנתונים האמיתיים. ניתן לשקול גם את האפשרות לתכנן את האסימון כדי להפוך אותו יותר שימושי. לדוגמה, ארבע הספרות האחרונות של מספר כרטיס האשראי יכולות להישמר באסימון, כך שניתן יהיה להדפיס את המספר המאוגד (או חלק ממנו) על קבלת הלקוח, כך שבפועל תוכל לראות הפניה למספר כרטיס האשראי של אותו צרכן. התווים המודפסים עשויים להיות כולם כוכביות בתוספת ארבעת הספרות האחרונות. במקרה זה, לסוחר יש רק אסימון, לא מספר כרטיס אשראי אמיתי, למטרות אבטחת המידע הרגיש (במקרה הזה, מספר כרטיס האשראי).

יתרונות השימוש בהצפנה וטוקניזציה

אחד המקרים הנפוצים ביותר לשימוש בטוקניזציה הינו הגנה על נתוני כרטיסי אשראי, כך סוחרים יכולים להפחית את התחייבויותיהם מבחינת עמידה בדרישות תקינה ורגולציות כגון PCI-DSS, GLBA, GDPR ועוד. ניתן להשתמש גם בהצפנה לצורך הגנה על כרטיסי אשראי, אך מכיוון שהנתונים עדיין קיימים כרגיל, רק תחת מעטפת הצפנה, הארגון חייב לוודא שכל התשתית הטכנולוגית המשמשת לאחסון והעברה של נתונים אלה תואמת באופן מלא את דרישות התקינה והרגולציה.

מועצת התקנים של תעשיית כרטיסי האשראי (PCI SCC) שמהווה את הסמכות המשפטית לאכיפת הרגולציה של ה-PCI DSS, פרסמה הנחיות לשימוש בטוקניזציה לצורך שמירה נאותה על נתוני כרטיסי אשראי. בעוד שהנחיות אלו עדיין לא נוספו באופן פורמאלי לדרישות התקן PCI DSS, הסוקרים (QSA) מקבלים כיום את השימוש בטוקניזציה כפתרון קיימא להגן בצורה נאותה גם על נתונים לא מובנים כדי לעמוד בדרישות התקן.

כיום, בעידן איומי הסייבר, יותר ויותר ארגונים מאמצים את השימוש באסימונים (טוקניזציה) כדי להבטיח גם סוגים אחרים של מידע כגון תעודות זהות, מספרי טלפון, כתובות דוא"ל, מספרי חשבון בנק, מספר רישוי רכב, ועוד.

מערכות ויישומים רבים בארגונים מסתמכים על מספרי ביטוח לאומי, מספרי דרכון ואף מספרי רישיון נהיגה כמזהים ייחודיים. מכיוון שמזהה ייחודי זה ארוג במערכות אלו, קשה מאוד להסירן או להצפין אותם. וגם מזהים אלה משמשים לגישה למידע רגיש אחר כגון חיוב הלקוח, סטטוס ההזמנה, ושירות לקוחות. ארגונים רבים משתמשים כיום בטוקניזציה כדי להגן על הנתונים הרגישים האגור במערכות אלו. השימוש בטוקניזציה מאפשר לארגון להמשיך לתמוך בפונקציונאליות של מערכת ה-Backend, מבלי לחשוף את הנתונים הרגישים (PII) בפני התוקפים.

אומנם אחד השימושים בהצפנה הינו גם לאבטח שדות מובנים בתוך בסיסי הנתונים, כגון פרטי כרטיסי אשראי, וחשבונות משתמשים (PII), היתרון בהצפנה הוא שזה מאפשר לשמור על פורמט הנתונים המקוריים, מה שמונע את הצורך לשנות את הסכמה של בסיס הנתונים ומאפשר שימוש בנתונים אלו ביישומים שונים ללא צורך בשינוי. לדוגמה, ניתן להצפין שדה שם מלא, כך שהערך המוצפן יישאר בפורמט של מחרוזת תווים, מה שיאפשר שימוש בו ביישומים שונים ללא צורך בשינוי.

הצפנה יכולה להתבצע ברמת שדה, קובץ או אפילו ברמת הדיסק כולו. הצפנה ברמת השדה מאפשרת הגנה גרנולרית על נתונים רגישים, בעוד שהצפנה ברמת הקובץ או הדיסק מספקת הגנה רחבה יותר על כל הנתונים המאוחסנים במערכת. הצפנה יכולה גם להגן על נתונים בתנועה, כאשר הם מועברים בין מערכות או דרך רשתות, מה שמבטיח שגם אם יירטו את הנתונים, הם יישארו בלתי קריאים ללא המפתח המתאים.

הצפנה יכולה להיות מיושמת בשכבות שונות של מחסנית הרשת, כגון שכבת היישום, שכבת התעבורה או שכבת הרשת. הצפנה בשכבת היישום מתמקדת בהגנה על נתונים ספציפיים, כגון הודעות דוא"ל או קבצים, בעוד שהצפנה בשכבת התעבורה מגנה על כל הנתונים המועברים בין שתי נקודות קצה, כגון לקוח ושרת. הצפנה בשכבת הרשת מספקת הגנה על כל התעבורה ברשת, כולל כותרות ומטא-נתונים.

הצפנה יכולה להיות מיושמת באמצעות מגוון אלגוריתמים, כל אחד עם חוזקות וחולשות משלו. אלגוריתמים נפוצים כוללים AES, RSA ו-ECC. בחירת האלגוריתם תלויה ברמת האבטחה הנדרשת, בביצועים ובתאימות למערכות ויישומים קיימים.

ניהול מפתחות הוא היבט קריטי של הצפנה, שכן אובדן או פגיעה במפתחות עלולים להוביל לאובדן נתונים או לגישה לא מורשית. ארגונים חייבים ליישם נהלים חזקים לניהול מפתחות, כולל יצירה, אחסון, סיבוב וביטול מפתחות. שימוש במודולי אבטחת חומרה (HSM) או בשירותי ניהול מפתחות מבוססי ענן יכול לעזור להבטיח את אבטחת המפתחות ולפשט את ניהולם.

הצפנה יכולה גם לעזור לארגונים לעמוד בדרישות רגולטוריות ותקנים בתעשייה, כגון GDPR, HIPAA ו-PCI DSS, על ידי הגנה על נתונים רגישים ומתן הוכחה לאמצעי אבטחה נאותים במקרה של הפרת נתונים או ביקורת.

עם זאת, חשוב לציין כי הצפנה אינה פתרון קסם ואינה מגנה מפני כל סוגי האיומים. היא צריכה להיות חלק מאסטרטגיית אבטחה מקיפה יותר הכוללת אמצעים אחרים, כגון בקרות גישה, ניטור ומודעות לאבטחה, כדי לספק הגנה מקיפה על נתונים רגישים.

הצפנה יכולה להיות מיושמת בשכבות שונות של מחסנית הרשת, כגון שכבת היישום, שכבת התעבורה או שכבת הרשת. הצפנה בשכבת היישום מתמקדת בהגנה על נתונים ספציפיים, כגון הודעות דוא"ל או קבצים, בעוד שהצפנה בשכבת התעבורה מגנה על כל הנתונים המועברים בין שתי נקודות קצה, כגון לקוח ושרת. הצפנה בשכבת הרשת מספקת הגנה על כל התעבורה ברשת, כולל כותרות ומטא-נתונים.

הצפנה יכולה להיות מיושמת באמצעות מגוון אלגוריתמים, כל אחד עם חוזקות וחולשות משלו. אלגוריתמים נפוצים כוללים AES, RSA ו-ECC. בחירת האלגוריתם תלויה ברמת האבטחה הנדרשת, בביצועים ובתאימות למערכות ויישומים קיימים.

ניהול מפתחות הוא היבט קריטי של הצפנה, שכן אובדן או פגיעה במפתחות עלולים להוביל לאובדן נתונים או לגישה לא מורשית. ארגונים חייבים ליישם נהלים חזקים לניהול מפתחות, כולל יצירה, אחסון, סיבוב וביטול מפתחות. שימוש במודולי אבטחת חומרה (HSM) או בשירותי ניהול מפתחות מבוססי ענן יכול לעזור להבטיח את אבטחת המפתחות ולפשט את ניהולם.

הצפנה יכולה גם לעזור לארגונים לעמוד בדרישות התקן.

כיום, בעידן איומי הסייבר, יותר ויותר ארגונים מאמצים את השימוש באסימונים (טוקניזציה) כדי להבטיח גם סוגים אחרים של מידע כגון תעודות זהות, מספרי טלפון, כתובות דוא"ל, מספרי חשבון בנק, מספר רישוי רכב, ועוד.

מערכות ויישומים רבים בארגונים מסתמכים על מספרי ביטוח לאומי, מספרי דרכון ואף מספרי רישיון נהיגה כמזהים ייחודיים. מכיוון שמזהה ייחודי זה ארוג במערכות אלו, קשה מאוד להסירן או להצפין אותם. וגם מזהים אלה משמשים לגישה למידע רגיש אחר כגון חיוב הלקוח, סטטוס ההזמנה, ושירות לקוחות. ארגונים רבים משתמשים כיום בטוקניזציה כדי להגן על הנתונים הרגישים האגור במערכות אלו. השימוש בטוקניזציה מאפשר לארגון להמשיך לתמוך בפונקציונאליות של מערכת ה-Backend, מבלי לחשוף את הנתונים הרגישים (PII) בפני התוקפים.

אומנם אחד השימושים בהצפנה הינו גם לאבטח שדות מובנים בתוך בסיסי הנתונים, כגון פרטי כרטיסי אשראי, וחשבונות משתמשים (PII), היתרון בהצפנה הוא שזה מאפשר לשמור על פורמט הנתונים המקוריים, מה שמונע את הצורך לשנות את הסכמה של בסיס הנתונים ומאפשר שימוש בנתונים אלו ביישומים שונים ללא צורך בשינוי. לדוגמה, ניתן להצפין שדה שם מלא, כך שהערך המוצפן יישאר בפורמט של מחרוזת תווים, מה שיאפשר שימוש בו ביישומים שונים ללא צורך בשינוי.

הצפנה יכולה להתבצע ברמת שדה, קובץ או אפילו ברמת הדיסק כולו. הצפנה ברמת השדה מאפשרת הגנה גרנולרית על נתונים רגישים, בעוד שהצפנה ברמת הקובץ או הדיסק מספקת הגנה רחבה יותר על כל הנתונים המאוחסנים במערכת. הצפנה יכולה גם להגן על נתונים בתנועה, כאשר הם מועברים בין מערכות או דרך רשתות, מה שמבטיח שגם אם יירטו את הנתונים, הם יישארו בלתי קריאים ללא המפתח המתא





בקרוב, שמאי סייבר?

ל-NIST יש מענה למלחמה במתקפות APT

הכירו את הסייבר רסיליינס



מאת: **עינת מירון**
יועצת מומחית
ליישום Cyber Resilience
מקבוצת סימנטיק.
www.meyron-mc.com
linkedin.com/in/einatmeyron

לפני 30 שנה חיינו כולנו בבתים עם חלונות ללא סורגים ואת דלת הבית טרחנו לנעול אם בכלל, רק בלילה כשכולם הלכו לישון. ואז גבים ניצלו את הפרצה קצת יותר מדיי וחברות ביטוח התחילו להתעקש על נעילת הדלת ואחכ על דלת פלדלת ואז הגיעו הסורגים והכספות.

מנכ"ל Aon אמר לאחרונה כי עלות פשעי הסייבר לארגונים היא 450 מיליארד דולר בשנה. מנהלת סיכונים סיפרה לי שהיא יודעת בודאות על פוליסות ביטוח סייבר ששולמו במלואן, בזמן אמת, ללא שאלות ובדיקות מעמיקות, רק בגלל ההבנה שככל שעובר הזמן מרגע המתקפה, היקף הנזק עלול להכפיל ולשלש את עצמו ולכן עדיף לשלם את התביעה מהר ככל האפשר.

איומי הסייבר הם כבר לא באזז וורד שמשתמשים בו להפחדה. הם מוחשיים והם עולים הרבה מאוד כסף. לארגונים שעובדים עם האיחוד האירופי, הם עלולים, החל ממאי2018, גם לעלות באחריות אישית של מנכ"ל החברה.

כיצד מתמודדים עם האיומים הללו? מלבד הגישות השמרניות שמאפשרות למנהל אבטחת המידע להוסיף עוד ועוד כלי הגנה, בעולם מתפתחת לאחרונה מגמה חדשה, Cyber Resilience, שמתייחסת לאיומי הסייבר כאיומים עסקיים לכל דבר. לחלוטין לא טכנולוגיים. איומים תפעוליים. אם נצא מנקודת הנחה שממונה הסייבר או מנהל אבטחת המידע יודע את עבודתו היטב אז מצב הארגון לא רע. אבל האם ממונה הסייבר מבין את מכלול השיקולים העסקיים? האם הוא יודע לשקף להנהלת החברה את הקושי הטכנולוגי שאיתו הוא מתמודד יחד עם ההשלכה העסקית? האם הנהלת הארגון יודעת איזה החלטות לקבל עם היוודע מימוש האיום?

מחקרים בעולם מעידים שלא. ישנו פער גדול מדיי בין הבנת האיומים לבין ההתמודדות איתם בפועל. הצורך לנהל תקשורת יעילה בזמן מתקפה מול הרגולטור, התקשורת, עובדי החברה, הספקים והלקוחות, היא כנראה האתגר הגדול ביותר שאיתו הארגון עדיין לא התמודד. וכשלא מנוסים בהתמודדות שכזו, היכולת לנהל אותה מלכתחילה סובלת מקשיים ובעיות.

חלק מהמתודולוגיה ההכרחית ביישום נהלי Cyber Resilience היא בהגדרה ובסיווג האיומים העלולים לשבש דרמטית את הארגון ועד לאלו שהם חלק מהשגרה המנוהלת. כאשר הארגון יודע מה נחשב לדרמה ומה לא, הגדיר צוותי תגובה שמודעים כל אחד לאחריותו ולפעילותו, שומר באופן רציף על קשר עם הרגולטור ועם CERT, ערוך עם תשובות וערוצי תגובה פתוחים למול התקשורת, הלקוחות והספקים הוא מצליח לנהל כמעט 75% מהנושאים שיידרש אליהם בזמן אמת.

ראינו כיצד ארגוני ענק כמו דלוייט, אקוויפקס, אובר ואלה הן רק כמה דוגמאות מהחודשים האחרונים, מאבדים את שיקול הדעת שלהם בהתמודדות עם מתקפת סייבר. חלקם מוכרים מניות, חלקם מסתירים מידע, חלקם משלמים כופר ומצניעים את המהלך. הביקורת הציבורית מכאיבה לכשעצמה, אבל היא בהחלט לא כאב הראש היחיד. חוסר האמון שנוצר משליך מיידית על המסחר במניה ועובר דרך סיקור תקשורתי מכביד ומביך יחד עם רעש עצום ברשתות החברתיות. אם נוסיף לזה גם עיצום כספי שמשית הרגולטור או התפטרות של מנהלים, כנראה שההבנה שנדרשת התייחסות אחרת היא בלתי נמנעת.

כשמיישמים מתודולוגיית Cyber Resilience, זה קצת כמו לתרגל גיוס מילואים ויציאה למלחמה. ארגון שלא תירגל, יופתע, יספוג נזקים כספיים ותדמיתיים כבדים. ארגון שיתרגל, ישמור על החוסן העסקי שלו ויידרש פחות לתביעות כספיות.

בעקבות גל המתקפות סייבר אשר פקד על ארה"ב בשנתיים האחרונות (ביניהם מתקפת הסייבר אשר השפיעה על הבחירות בשנת 2016), העלה את נוסא הסייבר רסיליינס לכותרות. המכון הלאומי האמריקאי לתקנים (NIST) פרסם לאחרונה טיוטה בשאיפה לסייע לארגונים להתמודד עם נקודות תורפה וליצור מערכות יותר מוגנות ובעלות שרידות גבוהה מפני מתקפות סייבר.

מדובר במסמך שנקרא Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems – והוא מספק הנחיות והמלצות לטיפול באיומי APT המכוונים לתשתיות IT במטרה לפגוע ביכולת הציפיות התפעולית של הארגון. המסמך ישים בעיקר למערכות חדשות שמפתחים, אך מתייחס גם לשיקולים הנדסיים בעת שיפור חוסן הסייבר במערכות Legacy.

NIST מגדירים את החוסן הקיברנטי (Cyber Resilience) כ"היכולת של הארגון לצפות אירועי סייבר, לעמוד בפני אירועי סייבר, להתאושש מאירועי סייבר ולהתאים את עצמו למצבי שליליים כגון מצבי לחץ, מתקפות סייבר או השתלטות על מערכות שעושות שימוש או מופעלות ע"י משאבי סייבר שונים ללא תלות במקור".

המסמך מתייחס למספר אלמנטים של עולם החוסן הקיברנטי כדי לספק מסגרת נאותה שתכלול מטרות, יעדים, טכניקות ושיטות, ועקרונות עיצוב מערכת בצורה מאובטחת.

עפ"י דבריו של רון רוס (Ron Ross), סוקר במכון NIST ואחד היוצרים של המסמך, "טיוטת המסמך מנחה את הארכיטקטים כיצד לאפיין ולפתח מערכות מאובטחות על ידי יצירת הבנה מובנית של דרישות המערכת, תוך התייחסות לכלל המרכיבים של המערכת, תהליכים ומשימות, כך שהארגון מייצר מערכות אמינות יותר מבחינת החוסן הקיברנטי שלהם, שמסוגלות לחלוטין לתמוך במשימות קריטיות ותהליכים עסקיים תוך הגנה על נכסי מידע קריטיים, ולעשות זאת בביטחון ובוודאות באותה רמה שעולה בקנה מידה אחד עם סובלנות הסיכון (Risk Appetite) של בעלי העניין בארגון".

ניתן להתייחס למסמך כאל מדריך הנחיות, וארגונים יכולים להשתמש בחלק או בכל העקרונות החוסן הקיברנטי המתוארים במסמך וליישם אותם בסביבות הטכנולוגיות, התפעוליות ובהתאם למתאר איומי הייחוס של הארגון.

על מנת להתמקד באופן ספציפי באיומי הייחוס של עולם החוסן הקיברנטי, על הארגונים:

- לשים דגש על הדרישות העסקיות הקריטיות לצורך עמידה ביעדי החברה
- לשים דגש על מידת ההשפעה של איומי ה-APT על הארגון, על מנת לייצר מערכות אבטחה שיכולות לחזות מתקפות סייבר, לעמוד בפני מתקפות סייבר, להתאושש ממתקפות סייבר ולהתאים את עצמה לכל מצב אסון או אירוע סייבר.
- להניח שהיריב יצליח לתקוף (להשתלט או לפגוע) מערכות ואף את הארגון עצמו, כדי למצוא ליקויים בסביבות התפעוליות ובשרשרת האספקה של הארגון.
- להניח שהיריב יהיה מסוגל לשמור על נוכחות במערכות או בארגון, באמצעות מימוש איומים שקשה למזער ולהעלים לאורך זמן.

כדי לסייע לארגונים לבנות חוסן קיברנטי לתהליכים השונים שבמחזור חיי מערכות המידע, המדריך מכיל הנחיות אודות הטמעה, אינטגרציה, זיהוי, מעבר, אימות, תפעול, תחזוקה וסילוק המערכת.

הציבור מתבקש ויוכל להעיר הערות לטיוטה זו עד לתאריך 18 למאי 2018.

5 סיבות

לאיבוד הכשרונות בתחום אבטחת המידע

ומה ניתן לעשות כדי לשמר אותם

אחד מהתהליכים המאתגרים והקשים ביותר בתחום משאבי האנוש בעידן הסייבר של היום הינו למצוא כישרונות חדשים, אבל לאבד את הכישרונות הללו לאחר שכבר השגת אותם יכול להיות לא פחות כואב.

אתגר #1

תקציב מוגבל ואסטרטגיה שלא תואמת את המציאות

לדברי גופי מחקר (אנליסטים), נמצא כי בערך 80% מהתקציב בתחום אבטחת המידע הולך לטובת ניסיונות למנוע את מתקפות הסייבר, בעוד שזה משאיר בערך 20% עבור אסטרטגיות לזיהוי ואיתור או ניסיונות לחזות מתקפות עתידיות. מדובר באיזון לא בריא בכלל, שיכול בסופו של דבר להוביל לשחיקה של עובד.

ותשאלו כל מומחה אבטחת מידע, והוא יגיד לכם את אותה תשובה: לא משנה כמה תשקיעו ותנסו למנוע את המתקפות, תמיד יהיו מתקפות שיצליחו. וכשזה קורה, זה חיוני ביותר שלארגון יהיה מערך נכון של ניטור, זיהוי ותגובה לאירועי אבטחת מידע.

ולכן, מומחים ממליצים לנוע בין 40%-60%, כאשר 60% מההשקעה יהיה לטובת פעולות מניעה, ו-40% מההשקעה תלך לטובת פעולות ניטור, זיהוי ותגובה לאירועי אבטחת מידע.

ביצוע שינוי זה לא מחייב אותך להגדיל את התקציב שלך, במקום זאת הוא מחייב אותך לשנות את חלוקת התקציב מבחינת סדרי העדיפויות שלו והקצאת כח אדם. שינוי זה יכול להשפיע גם באופן חיובי על תהליך שימור העובדים בארגון, כי עובדים מעדיפים להקדיש את זמנם על משימות אסטרטגיות וליזום משימות שדורשות חשיבה אסטרטגית ואנליטית (למשל ניתוח מודיעין סייבר, ניתוח וזיהוי פגיעויות, צייד איומים ועוד) מאשר להסתכל על מערכות הניטור ולבהות במסך באלפי הלוגים שמתרוצצים שם.

אתגר #2

הכשרה מקצועית, קידום קריירה ומנטורינג

בעיה זו אינה ייחודית לעולם אבטחת המידע, אבל בהחלט חלה גם על תחום זה באותה מידה. לעתים קרובות אנשים עוזבים את מקום עבודתם כי הם לא מרגישים שיש דרך ברורה לקידום או שמקום העבודה שלהם לא משקיע בהם על מנת לשפר או לשמר את הכשירות המקצועית.

בעולם אבטחת המידע, ישנם כמה דברים שניתן לעשות כדי לסייע לעובדים להרגיש כאילו הם חלק מוערך בצוות העבודה שלכם:

- תציעו הזדמנויות להכשרות מתמשכות: בין אם מדובר בלימוד בזמן ארוחות צהריים (Eat & Learn) ובין אם מדובר בהדרכות חיצוניות (שהארגון משלם עבורם), זה נותן לעובדים הרגשה שמשקיעים בהם ותומכים בהם על מנת לשפר את הכשירות המקצועית שלהם, וזה מעיד על הארגון כארגון תומך ורוצה להשקיע בקריירה של העובדים שלו.
- הצגה לעובדים של הנתיב לקידום מקצועי: חשוב לספק לעובדים כיוון ברור איך הנתיב קדימה נראה, ומהם צריכים לשאוף לעשות או להשיג על מנת להתקדם בסולם התפקידים. כל חברה שונה מהשנייה, ותלויה בתרבות הארגונית שלה, אבל ארגון שבו נתיב הקידום המקצועי ברור לעובדיו, הוא ארגון שיצליח לשמר את העובדים לתקופה ארוכה.
- הקצה מנחים מקצועיים (מנטורים): חשוב להקצות מנטורים לכל חבר בצוות, כזה שיוכל לשמש כמנטור אישי לכל בעיה שלא תהיה במהלך עבודתו. כך, העובד ירגיש שהוא לא אבוד, ויש לו למי לפנות במקרה שהוא נתקע. אותו מנטור אישי יכול לסייע לעובדים בליווי אישי, או בעיצות וטיפים כיצד להתקדם במקום העבודה או לבצע את התפקיד בצורה הטובה ביותר.

אתגר #3

צייד כשרונות

בהתחשב בפער העצום בין דרישות העבודה לכשרונות החדשים בשוק העבודה ולהיצע, ארגונים רבים מחפשים לנצל הזדמנויות "לחטט" בגינה של השכן, ולצוד כשרונות מחברות אחרות. אמנם זה יכול לשחק לטובתכם, זה יכול לשמש גם כנגדכם, באם חברות מתחרות יתחילו לצוד לכם עובדים.

כדי לסייע בהגנה על החברה מפני צייד עובדים, ולחזק את תהליך שימור העובדים בארגון עליכם:

- לשים לב לעלייה במשכורות במשק ושאפו לשמור על הקצב: אם הכשרונות הטובים שלכם עלולים לקבל שכר גבוה יותר בחברות המתחרות, אולי כדאי לכם לשקול להשוות את השכר, על מנת לשמר אותם, ולא להיקלע למצב שבו אתם גם נמצאים במחסור עובדים, וגם משקיעים כסף בניסיונות גיוס עובדים חדשים.
- הפכו את הארגון שלכם למקום שבו העובדים מוערכים עבור העבודה שהם עושים: תנסו להעריך את העבודה שלכם, ולהציג את זה בפניהם, בכל צורה שהיא. תודות וברכות באתר החברה, באו באירועי החברה על פרויקטים ומשימות או הצלחות הינה דרך אחת לחזק את ההערכה של הארגון כלפי העובד. למשל, אנחנו בטיטנס מנצלים את הבמה של המגזין כדי לחשוף את הכשרונות שלנו, שמשתפים אתכם את הידע והניסיון שלהם באמצעות פרסום הכתבות במגזין.



- תנו לעובדים משימות ופרויקטיים מהותיים: במידת האפשר, תנסו להעמיס את הלו"ז שלהם במשימות ופרויקטים שהם נהנים לבצע אותם. בלא מעט מקרים, כאשר עובדים נוטשים את מקום העבודה שלהם, לא מדובר בכסף, אלא במהות ומשמעות של התפקיד, או קידום מקצועי ועניין רב בפרויקטים חדשים. מדובר בהגשמה עצמית, ולכן חשוב לחזק את העובד ולספק לו עבודה שהוא נהנה ומסוגל לבצע. למשל: הגדירו היטב את המשימות שעל העובד לבצע, תוך קביעת מדדים ברורים למדידת ההצלחה והאפקטיביות של הפרויקט, ותוודאו שלעובדים יש את הכלים הנכונים (ידע, יכולת, ניסיון, זמן) כדי לבצע את העבודה.

אתגר #4

דרישות פרודוקטיביות גבוהות

בסקר שנערך ע"י המגזין הבינלאומי Computerworld, עולה כי 65% מהעובדים בתחום אבטחת המידע מתבקשים להגדיל את התפוקה שלהם במהלך השנה, ולקחת על עצמם יותר אחריות, בעוד ש-80% מהעובדים טענו לכך שהשכר שלהם לא השתנה כדי לפצות אל מול הדרישות הגבוהות מצד דרישות התפקיד.

מדובר באתגר לא פשוט מצד מנהלי הגיוס וציידי הכשרונות, שמצד אחד ישנה דרישה ההולכת וגוברת מבחינת היכולות של העובדים, ומצדו השני של המטבע עניין השכר אינו גמיש. כמובן שאתם רוצים לשלם לכולם יותר, אבל זה לא תמיד מציאותי.

בנוסף, השילוב בין הציפיות של הגדלת התפוקה ועליה בפרודוקטיביות של העובד לבין הנפח ההולך והגובר של כמות העבודה שעל העובד לבצע עלול לגרום סדקים בתקרת הזכוכית שלכם, ולבסוף לשחיקה של העובד.

אתם חייבים למצוא את האיזון הנכון בין העליה הנדרשת ברמת הפרודוקטיביות, לבין העניין הרב בתפקיד מבחינת משימות ופרויקטים חדשים או מעניינים, או לפחות לתגמל את זה באופן פיננסי, באמצעות עליה בשכר.

תזכרו שמרבית העובדים לא מונעים רק מדרישות השכר, אלא גם מהגשמה עצמית, רצון להתפתח מקצועית וניהולית, להוביל ולהוות מנטור או בעל השפעה מהותית בחברה.

כדי להתמודד בצורה נאותה עם הלחצים של הציפיות בעליה בתפוקה השנתית, יש לבחון שינוי אסטרטגי בתהליכי העבודה בארגון. למשל, מימוש תהליכים אוטומטיים במשרות מסוימות (כגון בקרים ב-SOC, אנליסטים, צוותי תגובה, וכדומה), או חלוקה שווה בשווה בין חברי הצוות, או שינויים ארגוניים שיכולים להקל על חלוקת העומס.

כמו כן, תנסו לייעל תהליכי עבודה שהיו לוקחים זמן רב, אולי בשינוי תהליך העבודה כפי שהוא מתבצע היום, או למכן אותו. זה יאפשר לעובדים זמן פנוי לקידום אישי ומקצועי, מה שיכול לתרום להם בדרך להגשמה העצמית שלהם.

אתגר #5

שמירה על מצבור של מועמדים

כמובן, אובדן כישרון מסוים הוא לעתים בלתי נמנע. אבל זה בדיוק למה אתם צריכים לשמור מצבור מלא של מועמדים כדי לסייע בתהליך הקליטה ומילוי החורים של המשרות במקום הכשרונות שאבדו. הנה כמה דרכים לעשות זאת בצורה נבונה:

- השתתפו בכנסים ותחרויות בתחום אבטחת מידע: השתתפות בכנסים, ימי עיון, ותחרויות (האקתון) בתחום אבטחת מידע מהווה דרך מצוינת להגדיל את החשיפה עבור החברה שלכם, תוך היכולת של ציידי הכשרונות שלכם לזהות ולאמוד כשרונות חדשים באווירה פתוחה וידידותית.
- להעביר הרצאות באוניברסיטאות או מכללות: חשיפה בפני קהל רחב של סטודנטים יכול לחשוף אתכם לקהל רחב של מועמדים ראויים למשרות התמחות בחברה שלכם, שלאחר תקופת ההתמחות יכולים להישאר כעובדים מן המניין. בנוסף, זה נותן לכם חשיפה ובמה לשווק את מובילי הדעה והמומחים שלכם על במות שונות ברחבי הארץ.
- הרחבת החיפושים אחר מועמדים: תזכרו תמיד להסתכל פנימה, לפני שאתם מסתכלים החוצה. האם יש מישהו אצלכם בארגון, אשר נמצא בעמדה נחותה ואשר יכול למלא תפקיד אחר, טוב יותר עבורו ועבור הארגון? או מישהו שעובד בתחום אחר שמשיק לעולם אבטחת המידע, אבל ניחן בתכונות וניסיון וידע או יכולת למלא אחר תפקיד אחר בתחום אבטחת המידע? שינוי תפקיד יכול לסייע לארגון הן מבחינת חסכון במשאבי הגיוס וההשמה, והן מבחינת שימור עובדים, בכך שעובד כעת מנויד לתפקיד אחר, שהוא חושק בו יותר, ויכול לתרום הרבה יותר לארגון. כעת העובד עם מוטיבציה גבוהה יותר, והארגון חסך כסף מיותר בתהליך השמה.
- תשמרו על תהליך גיוס מתמיד: גייסו מנהל או מנהלת גיוס אשר תפקידם יהיה להתעסק באופן שוטף עם תהליך הגיוס בחברה. חשוב שהם יהיו מחוברים לתחום שלכם, ויבינו את הצרכים ואת ה-DNA של החברה. גם אם אין כרגע משרות פתוחות, עצם העובדה שמנהלת הגיוס נמצאת בקשר רציף עם מועמדים פוטנציאלים בתחום אבטחת המידע, מחזק את הקשרים הבין-אישיים ויכול לסייע בעתיד בגיוס נכון.

חשוב לגייס את האנשים הנכונים עבור המשרות הנכונות

עצה אחת אחרונה שאני מציעה לכם היא לשכור את האנשים הנכונים עבור המשרות המתאימות. בדרך זו, אתם מונעים את התסכול של ציפיות לא ברורות או מיומנויות לא רלוונטיות מצד המועמדים.

לשם כך, חשוב מאוד לדעת את הדברים הבאים:

- אילו סוגי תפקידים אתם צריכים למלא?
- איך נראים המועמדים האידיאליים?
- על מה אי אפשר להתפשר מבחינת דרישות התפקיד?
- מהי הגדרת התפקיד של המועמדים, כולל אחריות וסמכויות
- מהן המטרות הארוכות טווח מבחינת הקריירה של המועמדים וכיצד המשרה הזאת עוזרת להם לממש את מטרותיהם

בחברת TS-HR פיתחנו מדריך (eBook) דיגיטלי על תהליך גיוס מועמדים בתחום אבטחת המידע. במדריך אנחנו דנים על מגוון תפקידים בתחום אבטחת המידע, מהם דרישות התפקיד, אחריות, סמכויות, ניסיון, מהם המאפיינים העיקריים שחשוב שנחפש במועמדים, ורעיונות נוספים לגיוס ושימור עובדים.

למידע נוסף, תוכלו לגלוש באתר שלנו בכתובת www.titans2.com , או לפנות אלינו במייל: info@titans2.com

האיגוד העולמי לאבטחת מידע (ISSA) –הצ'אפטר הישראלי

ISSA™
Information Systems Security Association
The Global Voice of the Information Security Profession

האיגוד הינו גוף מלכ"ר (ללא מטרות רווח) כאשר מטרתו העיקרית היא קידום נושא אבטחת המידע בישראל, בכל ההיבטים.

חברי האיגוד נהנים מהטבות ייחודיות במהלך כל השנה, כגון הרצאות מקצועיות, ימי עיון, חומרים מקצועיים, ועוד. כיום, חברים באיגוד כמה מאות מקצועני אבטחת מידע, ואנו שואפים לגייס את כלל קהילת ה-IT בישראל. בנוסף, חברי האיגוד נהנים ממהדורה ייחודית ובלעדית של Global Security– המגזין המוביל בישראל בתחום אבטחת המידע.



אודות גיליון Global Security

למה כדאי לחפש מידע במגזין שלנו ולא למשל ב-Google או כל עיתון אחר?

- **מיקוד בתחום אבטחת המידע** – המגזין עוסק אך ורק בתחום אבטחת המידע וניהול סיכונים.
- **יותר כתבות מקצועיות ופחות תדמיתיות** – רוב המגזינים כיום יותר תדמיתיים, ופחות מקצועיים. אנו שומרים על רמה מקצועית, וכמות מינימאלית של כתבות תדמית.

  השוואתיות – מאפשר השוואה פשוטה ואובייקטיבית בין הספקים והפתרונות.

  היקף מידע – תמונה רחבה יותר, ולא רק התמקדות בנושאים ספציפיים.
- **תשלום סמלי** – מדובר בעלות סמלית, והנכם מנויים למגזין אבטחת המידע המוביל בישראל
- **מקצועני אבטחת מידע** – כל הכותבים שלנו עוסקים בתחום אבטחת המידע למעלה מ-7 שנים, והם בכירים בתחום, ברמה העולמית.

אחת לרבעון – מוסף מיוחד

מה הערך המוסף שלנו?

בעת בחירת ספק (מערכת\מוצר) תהליך מכרז או בקשה למידע מתחיל בפנייה שלכם לכמה ספקים בהתאם להוצאת RFI/RFP מהחברה. אנו מרכזים עבורכם את כל המידע המקצועי המקיף ביותר, ובר השוואה אודות הפתרונות אבטחת המידע השונים, באופן שזה מכסה את כל השאלות המרכזיות הנשאלות בנוגע לפתרון אפשרי:

1. סקירה טכנולוגית רחבה אודות הפתרון שמחפשים
2. סקירת הפתרונות בתחום הספציפי.
3. מי הם הספקים המובילים בתחום?
5. פרטי החברה של היצרן/ספק/ האינטרגטור: שם, מספר עובדים, שנת הקמה, יתרונות וחסרונות, סוגי פעילות בחברה, נושאים \תחומי פעילות והתמחות, קישורים, מידע טכנולוגי, איש קשר, חוסן כלכלי, לקוחות בארץ, לקוחות בחו"ל, תוכניות הרחבה למוצר, מספר התקנות בארץ
6. מה הערך המוסף של כל ספק בתחום הפתרון המוצע?
7. כיצד מנהלים את הפרויקט?
8. מהם נקודות כשל בפרויקט שמהם צריכים להיזהר?
9. מה צריכים לדרוש מהספקים בעת יציאה למכרז?

CISM או CISSP?

מה ההבדלים ביניהם ולמי זה מתאים?



מאת: **דני אברמוביץ**
המנהל האקדמי של
TS-ACADEMY, מקבוצת
TITANS SECURITY

מחקרים שונים מראים כי הסמכות בינלאומיות בתחום אבטחת המידע מהווים יתרון מהותי במציאת מקומות עבודה ואף מסייעים בקידום במקום העבודה הנוכחי.

בעיני המעסיקים, בוגרי קורסים בעלי הסמכות בינלאומיות יותר אטראקטיביים מאשר מועמדים אחרים, היות וברחבי העולם, התקינה והרגולציות מחייבות ארגונים להעסיק מועמדים בעלי כשירות מקצועית והסמכות בינלאומיות שונות. ולכן, בוגרים בעלי הסמכות בינלאומיות מבדילים את עצמם משאר המועמדים, ומשפרים את הסיכויים שלהם להשיג משרות נחשקות יותר.

שתי ההסמכות הפופולאריות ביותר בעולם אבטחת המידע, הינן ה-CISM (ר"ת של Certified Information Security Manager) וה-CISSP (Certified Information System Security Professional). שתי ההסמכות דורשות ניסיון ומאמצים רבים על מנת להשיג אותן.

CISM או CISSP?

אז מהי כל הסמכה, ואיזה מהן יכולה להתאים לכם יותר? שתי ההסמכות משכו את תשומת ליבם של מעסיקים רבים בשנים האחרונות, והפכו להיות ההסמכות הפופולאריות ביותר בתעשייה. שתי ההסמכות ניתנן ע"י גופים ניטראליים, שלא מייצגים שום ספק מוצרים (Vendors), ודורשות ידע וניסיון בתחומים שונים בתחום אבטחת המידע.

CISM

ההסמכה של CISM, הינה הסמכה מבית ISACA (ר"ת של Information Systems Audit and Control Association) או בעברית פשוטה, האיגוד העולמי לביקורת ואבטחת מערכות מידע. ההסמכה מיועדת בעיקר למנהלי אבטחת מידע, או ליועצים שעוסקים יותר בעולם ה-GRC, ומספקים ייעוץ לארגונים ולמנהלי אבטחת מידע בנושאים כגון אסטרטגיה, מדיניות, מסגרות לניהול אבטחת מידע, ניהול סיכונים והלימה לתקינה ורגולציות שונות. ההסמכה שמה דגש רב על הקשר ההדוק לחיבור בין אבטחת המידע לפעילות העסקית של הארגון.

ההסמכה כוללת 4 מודולים עיקריים, שמתפרסים על הנושאים הבאים:

- **מודול 1**: ממשל אבטחת מידע
- **מודול 2**: ניהול סיכונים
- **מודול 3**: פיתוח וניהול תחום אבטחת המידע בארגון
- **מודול 4**: ניהול אירועי אבטחת מידע



כבסיס להסמכה, ישנה דרישה של 5 שנות ניסיון בשניים או יותר מהדומיינים שמפורטים לעיל, כאשר ניסיון של שנתיים לפחות בתחום ניהולי (מנהל אבטחת מידע).

ההסמכה של CISM מוכרת בארה"ב ע"י משרד ההגנה (ה-DOD), וע"י קונצרן ה-ISO העולמי.

ההסמכה שמה יותר דגש על מונחים טכנולוגיים, ולכן מי שמעוניין בהסמכה של ה-CISM, חייב לשלוט בנושאים העיקריים שההסמכה הזאת דורשת, על מנת לעבור את הבחינה בהצלחה.

תהליך קבלת ההסמכה מותנה בשני חלקים עיקריים: מעבר של בחינת ההסמכה , וסיום תהליך הכשר (Endorsement). שתי הכללים הללו מאפשרים למועמד לקבל את התעודה הנחשקת.

את התעודה חובה לתחזק, באמצעות שמירה על כשירות מקצועית, כלומר, במהלך כל שנה, על מחזיקי ההסמכה לשלם דמי חבר של 45 דולרים ל- ISACA, ובנוסף לצבור נקודות CPE (ר"ת של Continuing Professional Education). עליכם לבצור 120 נקודות זכות במהלך 3 שנים.

למידע נוסף אודות הדרישות של ההסמכה, ניתן לעיין באתר של ISACA בכתובת:
http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/FAQs.aspx

CISSP

ההסמכה של CISSP הינה הסמכה מבית ISC2 (ר"ת של International Information System Security Certification Consortium) או בעברית פשוטה, האיגוד העולמי להסמכות בתחום אבטחת מערכות מידע. להבדל מההסמכה של CISM, הסמכה זו מיועדת לקהל רחב יותר, כגון מנהלי אבטחת

מידע, יועצים, מנמ"רים, מנהלי IT, מהנדסי Pre-Sale, אינטגרטורים, מומחי אבטחה ובעלי תפקידים אחרים בתחום אבטחת המידע, שכמובן עובדים בדרישות הסף. ההסמכה מכילה יותר היבטים טכנולוגיים מאשר ההסמכה של ה-CISM, ולכן מיועדת לקהל רחב יותר.

ההסמכה כוללת 8 מודולים עיקריים, שמתפרסים על הנושאים הבאים:

- **מודול 1**: ממשל אבטחת מידע וניהול סיכונים
- **מודול 2**: ניהול נכסי מידע
- **מודול 3**: אבטחת מידע בהיבט הארכיטקטורה והנדסה
- **מודול 4**: אבטחת מידע ברשתות תקשורת
- **מודול 5**: בקרת וניהול זהויות
- **מודול 6**: בדיקות אבטחת מידע
- **מודול 7**: תפעול מערך אבטחת המידע
- **מודול 8**: אבטחת מידע בהיבטים של פיתוח תוכנה

כבסיס להסמכה, ישנה דרישה של 5 שנות ניסיון בשניים או יותר מהדומיינים שמפורטים לעיל, או ארבע שנים ותואר אקדמי רלוונטי.

הקהל יעד העיקרי להסמכת CISSP הינם בעיקר אנשי IT, אנליסטים, מומחי אבטחת מידע, ארכיטקטים, יועצים, מבקרים (סוקרים), מהנדסי מערכת ומנהלי אבטחת מידע.

גם ההסמכה של CISSP מוכרת בארה"ב ע"י משרד ההגנה (ה-DOD), וע"י קונצרן ה-ISO העולמי.

ההסמכה שמה יותר דגש על מונחים טכנולוגיים, ולכן מי שמעוניין בהסמכה של ה-CISSP, חייב לשלוט בנושאים העיקריים שההסמכה הזאת דורשת, על מנת לעבור את הבחינה בהצלחה.

תהליך קבלת ההסמכה מותנה בשני חלקים עיקריים: מעבר של בחינת ההסמכה , וסיום תהליך הכשר (Endorsement). שתי הכללים הללו מאפשרים למועמד לקבל את התעודה הנחשקת.

את התעודה חובה לתחזק, באמצעות שמירה על כשירות מקצועית, כלומר, במהלך כל שנה, על מחזיקי ההסמכה לשלם דמי חבר של 85 דולרים ל-ISC2, ובנוסף לצבור נקודות CPE (ר"ת של Continuing Professional Education). עליכם לבצור 120 נקודות זכות במהלך 3 שנים.

הבחינה עברה שינוי, וכעת היא 150 שאלות (במקום 250 שאלות כמו בעבר), ומתפרסת על כ-3 שעות. שינוי מהותי נוסף, הוא בכך שהבחינה כעת היא מתבצעת בשיטת CAT (ר"ת של Computer Adaptive Questions) , כלומר הקושי של השאלות עולה עם הזמן, בהתאם למה שעונה המועמד.

למידע נוסף אודות הדרישות של ההסמכה, ניתן לעיין באתר של ISC2 בכתובת:
https://www.isc2.org/Certifications/CISSP

אז על מה ללכת?

שתי ההסמכות אינן שמות דגש על טכנולוגיה או מוצר ספציפי, אלא מתייחסות באופן כללי לתחום אבטחת המידע.

ההסמכה של CISM מיועדת יותר למנהלי אבטחת מידע, או לבעלי תפקידים ניהוליים בתחום אבטחת המידע, בעוד שההסמכה של ה-CISSP מיועדת בעיקר ליועצים, מהנדסים Pre-Sale ואינטגרטורים.

כמובן, שכל אחד שעומד בדרישות הסף (ללא קשר לתפקידו הנוכחי), יכול לגשת לבחינה, ובמידה ויעבור את הבחינה בהצלחה, ואת תהליך ה-Endorsement – לקבל את ההסמכה הנחשקת.

בעולם, שתי ההסמכות זוכות להכרה מהותים, הן מצדם של המעסיקים, והן מצדם של התעשייה.

מחקרים שונים, מראים כי בעלי הסמכה של CISM נשכרים בשכר גבוה יותר, אבל זה בגלל תפקידם כמנהלי אבטחת מידע.

ההסמכות מוכיחות כי המועמדים בעלי כישורים בסיסיים שנדרשים למלא תפקידים מסוימים, ומאפשרים למועמדים לשוחח באותה שפה עם הקולגות בתעשיית אבטחת המידע.

עבור מעסיקים, נושא ההסמכה מהווה צעד נוסף בתהליך הסינון עובדים. ישנם מעסיקים שדורשים מראש בעלי הסמכה של CISSP, CISM או שתיהן, ולכן, קל יותר למעסיק לבצע סינון מבין עשרות או מאות מועמדים.

חשוב להבין, שההסמכה אינה מבטיחה הצלחה בתפקיד, אלא מאותת על כך שהמועמד בעל ידע בסיסי שעומד בדרישות הסף של התפקיד. מבחן התוצאה, יהיה במהלך התפקיד עצמו, תקופת ניסיון שבה על המעסיק לבחון את הכשירות המקצועית בפועל של אותו מועמד.

המלצותינו, היא לבחון את הכיוון בקריירה שאתה רוצים, האם אתם נמצאים בנקודת זמן שבה אתם רוצים להשקיע יותר לכיוון הניהולי, ואז ההסמכה של ה-CISM יכולה להתאים לכם יותר, או האם אתם רוצים להמשיך בתחום הייעוץ , ואז ההסמכה של ה-CISSP יכולה להתאים לכם יותר.

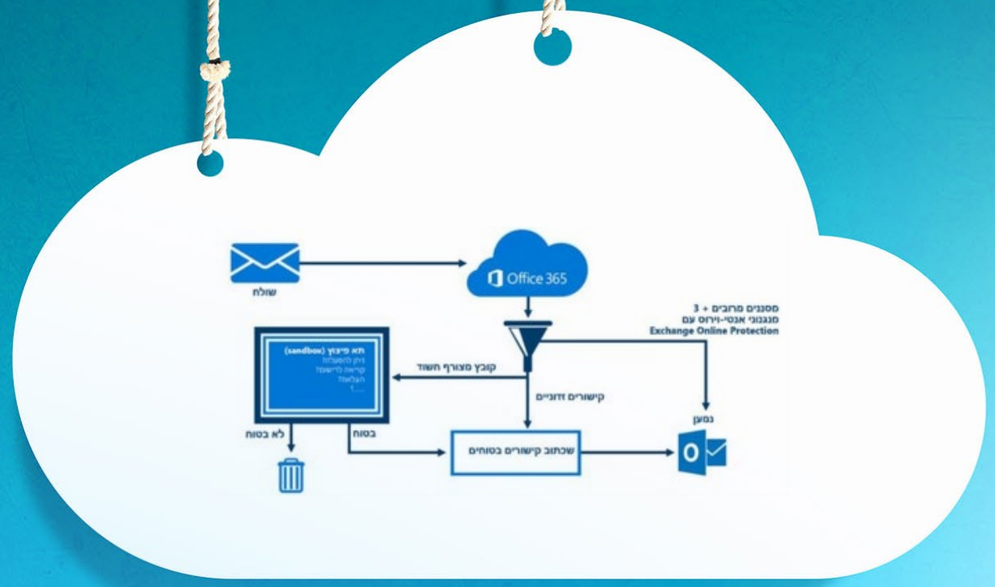
בכל מקרה, מניסיון בארץ ובעולם, מרבית האנשים במשק, עושים את שתי ההסמכות, במטרה לשפר את סיכויים להשגת תפקיד נחשק יותר, במקום הנוכחי, או במקום עבודה עתידי.

עננים מאובטחים



מאת: **שלומי מרדכי**, סמנכ"ל טכנולוגיות המידע בקריה האקדמית אונו, והמשנה לנשיא האיגוד העולמי לאבטחת מידע (ISSA) -הציאפטר הישראלי

הכירו את ה-ATP (Advanced Threat Protection) מבית מיקרוסופט פתרון מבוסס ענן, למניעת מתקפות ופרצות בשירותי הדוא"ל, התמודדות עם מתקפות Zero Day וקישורים זדוניים בתשתיות הדוא"ל.



בעידן הדיגיטלי של היום, מרבית הארגונים הוציאו את מערכות הליבה שלהם לענן, ביניהם יישומים כגון CRM, ERP, ואף הדואר האלקטרוני. אבל לעתים, מועבר במיילים גם מידע רגיש. מנהלי אבטחת המידע וצוותי ה-IT בארגון מתבקשים להתמודד עם התקפות ופרצות בשירותי הדוא"ל, אשר מערכות הסינון דואר הסטנדרטיות אינם יכולים לתת להם מענה. בנוסף, ישנן דרישות אבטחה נוספות כגון היכולת להתמודד עם מתקפות של העברת תוכן זדוני אשר עדיין לא מופו ואין להם חתימות זיהוי (מתקפות Zero Day).

לאחרונה אנו עדין ליותר ויותר מתקפות מתוחכמות אשר מצליחות לעבור בקלות את מנגנוני האבטחה הסטנדרטיים. פתאום אתם מגלים שיש פרצה בשירותי הדואר או התקפה זדונית על המערכת – והמיילים שלכם מגתלגלים הלאה, חשופים לעיני כל. מה עושים עכשיו?

אז מהו ה-ATP?

ה-ATP (ר"ת של Advanced Threat Protection) הוא שירות ענן עצמאי, הניתן להטמעה כחלק מתשתית ה-Office365. השירות מהווה נדבך נוסף מעל תשתית הסינון הבסיסית של ה-Office365 המבוססת על ה-EOP (Exchange Online Protection) מערכת המציעה שירות אנטי-וירוס רב-שכבתיים (Multi-Engine Anti Malware) ושירותי סינון דואר זבל (Anti-Spam)

השירות פותח על מנת לאפשר התמודדות עם מתקפות שמערכות סטנדרטיות לסינון דואר לא מכירות ולא יודעות להתמודד איתן כגון:

- תוכנות רוגלה או תוכנות זדוניות אחרות אשר טרם זוהו ולכן גם טרם הוגדרו להן חתימות במערכות הסינון (מה שקרוי מתקפות Zero Day).
- קישורים שנשלחים במייל ומעבירים לאתרים שנראים לכאורה לגיטימיים, אולם בפועל בכל נקודת זמן עלולים להפוך לאתרים זדוניים שמטרתם לבצע פישינג, לדלות מידע חשוב, לגנוב זהויות ו/או להדביק את מחשבי המשתמשים בתוכנות זדוניות אחרות.

בממשק ייעודי, ניתן לנהל את הכלים שתוסף זה מעניק לכם כדי ליצור כללים חדשים, לעקוב אחרי פעילויות חשודות, ליצור הגנה בזמן אמת, להיעזר בטכנולוגיה המתקדמת של זיהוי תקיפות בלתי מוכרות ועוד.

את היכולות המובנות של ה-Office365 כולנו כבר מכירים:

- מנגנון ה-EOP: ר"ת של Exchange Online Protection, מנגנון המספק הגנה מתקדמת מפני הודעות זבל ותוכנות זדוניות.



- מנגנון אנטי-וירוס: מנגנון הסורק באופן אקטיבי את ההודעות הנכנסות, היוצאות ואלו שכבר הגיעו לתיבת הדואר.
- מנגנון אנטי-ספאם: מנגנון הדואג לכך שבנוסף להגנה מפני דואר זבל נכנס, תיבת הדואר שלכם לא תהפוך למפיצת ספאם ללא ידיעתכם ומבצע בקרה והגבלה על התוכן הנשלח לנמענים.

תוסף ה-ATP עונה על צרכים מתקדמים יותר של הגנה על תשתיות הארגון, מתוך הבנה שעולם התקיפה הוירטואלי מתפתח ללא הרף ומתדבק על ההגנות הקיימות, הופך למתוחכם וחכם יותר מרגע לרגע.

תשתית ה-ATP מאפשרת זיהוי וירוסים ותוכן זדוני אחר בזמן אמת, גם ללא חתימות (מה שקרוי Zero Day Attacks) באמצעות מערכת בדיקה המריצה את הקודים בצורה חייה על גבי תשתית ענן מאובטחת (Sandbox) ומערכת סריקה ובדיקת קישורים המגיעים במייל (URL Reputation Filter).

מערכת בדיקת הקישורים למעשה עושה בדיקת Reputation לקישורים ומאפשרת או חוסמת את הגישה אליהם בזמן אמת. על מנת למנוע מקרה בו קישור תקין הופך לזדוני, המערכת מחליפה את הקישורים כל שכל פניה לקישור עוברת דרך תשתית הסינון, בדרך זו הקישור נבדק לא רק בזמן הגעת המייל אלא בכל נקודת זמן לאחר מכן בה לוחץ המשתמש על הקישור המופיע במייל

איך זה עובד?

להלן כמה מהתכונות הבולטות של השירות ATP:

- הגנה מפני קבצים לא בטוחים: קבצים מצורפים לא בטוחים מועברים לסביבה מבודדת (Quarantine) בתוך סביבה בטוחה ומבודדת (Sandbox) לפני שהם נשלחים לנמען, שם הם נבדקים ונסרקים לפני שמועברים לתיבת הדואר.
- הגנה מפני קישורים לא בטוחים: כתובת URL שנשלחת, נבחנת בזמן אמת מיד כשהמשתמש לוחץ עליה. במידה והקישור לא בטוח, קופצת הודעת אזהרה או הודעה שהאתר נחסם. ניתן גם להגדיר, למשל, שישלח דיווח למנהל המערכת כדי לראות איזה משתמש לחץ על הקישור ומתי.
- ניתוח איומים חדשים: כל ההודעות והקבצים המצורפים שאין להם חתימה ידועה של וירוס (או צורות תקיפה אחרות), מנותבים לסביבת Hypervisor מיוחדת, כאשר ניתוח ההתנהגות מבוצע תוך שימוש במגוון טכניקות של למידה ומכוונות לזיהוי כוונות זדוניות. אם לא זוהתה פעילות חשודה, ההודעה נשלחת למסירה לתיבת הדואר של הנמען.

מה כוללת המערכת?

המערכת כוללת מגוון יכולות ושירותים שחיוניים על מנת להגן על תיבת הדואר האלקטרוני וכפועל יוצא, על מחשבי הארגון ותקינות הרשת:

- סינון תוכנות זדוניות בזמן אמת
- מערכת Sandbox להרצת קודים (זדוניים)
- מערכת לבדיקת מוניטין (reputation) של קישורים המגיעים במייל
- יכולות אבטחה נוספות מובנות
- תמיכה בדרישות תקינה ורגולציות
- מערכת ניהול עומסים
- שרידות מובנית
- עדכוני גרסה שוטפים
- ועוד

הכירו את ה-CHATOPS

הכלי שיסייע לאנליסטים להתמודד בצורה יעילה יותר עם מתקפות סייבר



ה-ChatOps מהווה מודל לשיתוף מידע בין מרכיבים שונים כגון אנשים, כלים, תהליכים ואוטומציה, וכל זה באמצעות תהליך זרימה שקוף לחלוטין. מודל זה מחבר בין העבודה הנדרשת, לעבודה המתרחשת בזמן אמת, ולעבודה שמתבצעת באופן מתמיד באמצעות אנשים, בוטים וכלים ייעודיים. השקיפות מקצרת את תהליך המשוב, משפר את תהליך שיתוף המידע ומגביר את שיתוף הפעולה בין חברי הצוות. כמובן ישנם יתרונות נוספים כגון שיפור התרבות הארגונית לעבודה בצוות, והכשרות הדדיות מבין חברי הצוות השונים.

תשתיות ה-ChatOps כבר תפסו תאוצה באולם ה-DEVOPS כבר מזמן, וכעת זה משמש גם לתחום ניהול ותגובה לאירועי אבטחת מידע, בחמ"לים ובמרכזים לניהול אירועי אבטחת מידע (SOC). תשתית זו מאפשרת לצוותי התגובה (בתוך הארגון ומחוץ לארגון) לתקשר ולשתף מידע באופן מיידי, קל ויעיל.

כיום, ארגונים רבים משתמשים בתשתית ה-ChatOps לצורך אוטומציה של ניהול ותגובה לאירועי אבטחת מידע, למשל: מערכת התראות תשלח הודעה (התראה) על אירוע או תקרית אבטחת מידע אשר זוהה באחת מהמערכות בארגון, וכתגובה, הסוכן צי'אט יריץ פקודה (script) אשר הוגדרה מראש ע"י צוות התגובה ב-SOC.

בגדול, הארגונים משתמשים בתשתית זו כדי לסייע לצוותי אבטחת המידע לשתף פעולה, לחלוק מידע, ולבצע אוטומציה להיבטים המבצעיים של תהליכי גילוי ותגובה לאירועי תקיפה, וזה באמצעות שימוש בממשק של תשתית ה-ChatOps. תשתית זו באה לתת מענה לאתגרים התפעוליים שנגרמים בארגונים רבים כתוצאה מריבוי-יתר של כלים לא מקושרים וממחסור בכח אדם מיומן, אשר גוררים אי-עמידה בעומס בהתרעות וטיפול לא יעיל באירועי סייבר.

כיצד שימוש ב-ChatOps יכול למזער את ה-MTTR ב-SOC

לפני השימוש ב-ChatOps ניתן היה לומר שצוותי התגובה ב-SOC דשדשו בחול טובעני.

אחד האתגרים הנפוצים ביותר של אנליסטים בתחום אבטחת המידע הוא הזמן שנדרש כדי להגיב בהצלחה ולסגור אירוע. האיטיות בתגובה נובע מסיבות רבות, כגון: המספר העצום של אירועי אבטחת המידע שהאנליסטים צריכים להתמודד איתם, המעברים בין מוצרי אבטחת המידע השונים על מנת לחקור ולנתח את האירועים, והעובדה שהאנליסטים וצוותי התגובה עובדים בנפרד לפי שוללת מהם את האפשרות לעבוד ביחד ולשתף את הידע והניסיון שנצבר. לנוכח המצב הזה, ניתן לומר שצוותי התגובה והאנליסטים רצים במרתון...עם מגפיים שעשויים מבטון.

האיטיות בתהליך התחקור הדיגיטלי של האירוע נובע ממספר סיבות:

שיחות בתפזורת: כאשר האנליסטים וצוותי התגובה מגיעים למבוי סתום בעת תהליך תחקור אירוע, וצריכים עזרה, הם בד"כ מנסים להתייעץ עם קולגות לעבודה או לשאול בפורומים שונים באינטרנט. כאשר זה קורה, המון מידע שימושי הולך לאיבוד, בגלל תופעת "שיחות מסדרון", כי אין רישום ותיעוד מסודר של השיחות הללו.

מלבד הזמן שנדרש עבור האנליסטים וצוותי התגובה להתייחס למקורות המידע השונים הללו במהלך התחקור הדיגיטלי של האירוע, בזמן נוסף מבוזבז תוך איסוף כלל המידע מהמקורות הללו לצורכי קורלציה ואנליזה של כלל המידע.

מרוב עצים לא רואים את היער: בעת תחקור דיגיטלי של אירוע, לעתים קרובות, אנליסטים משתמשים במגוון כלים ומערכות אבטחה שונות שעומדות לרשותם ב-SOC. מערכות אלו מסייעות לאנליסטים בביצוע פעולות שונות, איסוף מידע, והרצת שאילתות שונות או שילוב של שלושתם. על מנת לעבוד עם כלל הכלים והמערכות הללו, לרוב, האנליסטים פותחים המון חלונות (tabs) במחשב האישי שלהם, אשר מתפרסים על מספר מסכים, במטרה להיכנס לכל מערכת בנפרד ולבצע את הפעולה הרצויה הרלוונטית.

זמני תגובה ארוכים: כל זה מוביל לעיכוב משמעותי בזמני התגובה (מה שידוע במונח dwell time), במיוחד במהלך חקירות ארוכות המחייבות שימוש במגוון רחב של מוצרים ומערכות אבטחת מידע (בין 10-15 מערכות שונות). זה גם מגדיל את הסיכוניים של טעויות אנוש היות ומצופה מהאנליסטים לבצע פעולות רבות בפרק זמן קצר, כגון משימות חוזרות (צפייה בלוגים שונים), פעולות העתק הדבק מכמה מערכות על הקונסול המרכזי, ולשמור תיעוד אודות כל מערכת ומערכת.

חסרונות אלו מגבירים את חרדת האנליסטים מהטיפול ותגובה לאירועי אבטחת מידע, ומסכנים את היכולת של הארגון לעמוד ב-SLA מבחינת פרק הזמן שצריכים לענות ולהגיב לכל אירוע אבטחת מידע, מה שיכול לגרום לשחיקה של האנליסטים ב-SOC.

אחרי ה-ChatOps – ניתן לומר שה-SOC הצטייד ביכולות ניטרו מה שמשפר מהותית את ביצועיו.

ניתן לומר שהשימוש ב-ChatOps פותר את כל שלושת הבעיות שהוזכרו לעיל. השימוש בחלון אחד באופן יעיל מבטל את הצורך לעבור בין מסכים של מערכות שונות, הממשק של הציאט מאפשר ומעודד את האנליסטים וצוותי התגובה לעבוד ביחד ולשתף מידע וידע, והיכולות הללו מובילות לתהליך של מזעור משמעותי בכמות ההתראות אשר יתקבלו ב-SOC.

חשוב לזכור, שכל שנייה שבה הפעילות של הארגון מושבתת כתוצאה מאירועי סייבר, יכול להוביל להוצאות כספיות רבות, או לתוצאות הרסניות אחרות, כגון פגיעה בחיי אדם (באם מדובר על ארגון המספק שירותים לתשתית קריטיות), ולכן, השימוש ב-ChatOps יכול לשפר באופן משמעותי את תהליך התגובה לאירועי סייבר.

אז כיצד ה-ChatOps תורם לשיפור מהותי מבחינת הדיוק, ויעילות בתחקור האירוע?

נקודה מרכזית אחת לאיסוף וריכוז השיחות: אם הצוותים השונים ב-SOC (בקרים, אנליסטים, מהנדסי מערכת, צוות תגובה וכו') משתמשים ב-ChatOps, אז כולם יכולים לשוחח ולשתף מידע בחלון מרכזי אחד, מה שמעלים את הצורך בחיפוש אחר מקורות מידע שונים.

הכירו את ה-ChatOps

ל-ChatOps יש גם אפשרות להתממשק עם פלטפורמות למסרים מידיים אחרים כגון Slack, מה שיאפשר לשקף ולשכפל את השיחות בין הצוותים השונים, וימנע את הצורך בהעתק הדבק לצורך העברת המסרים לשאר הצוותים. לבסוף, אם עדיין יש הערות שנותרו במקומות שונים כגון תיבות דוא"ל, tickets, או כל מדיה אחרת, ניתן יהיה להעלות הכל לתוך מערכת ה-ChatOps ולנהל את זה בצורה מרכזית. כך, ה-ChatOps יהפוך להיות מאגר מידע מרכזי לכלל המידע שנוגע לתחקור האירועים.

ניהול המערכות מנקודה מרכזית אחת: במקום להיכנס לממשק הניהול של כל מערכת אבטחת מידע, להריץ את הפקודות הנדרשות ולהעביר את התשובות חזרה למסד נתונים מרכזי כלשהו, מערכת ה-ChatOps מאפשר לאנליסטים להריץ פקודות שונות בזמן אמת באמצעות קונסול מרכזי אחד. מערכות ה-ChatOps מגיעות עם מגוון כלי עזר שונים, כגון ה-Chatbots – שבעצם הם אלו שניגשים למערכות אבטחת המידע, מריצים את הפקודות הנדרשות , ומחזירים את התשובות לקונסול מרכזי אחד (במקום לרוץ מבין מסכים של מערכות שונות).

שיפור מהותי בדיוק התחקור של אירועי הסייבר: מלבד חסכון בזמן התגובה לאירועי סייבר, השימוש בממשק ניהול מרכזי אחד מאפשר גם לשפר באופן משמעותי את הדיוק של הטיפול באירוע. אם האנליסטים מתעסקים פחות במשימות יומיומיות שכיחות שגוזלות זמן רב, הם נוטים פחות לבצע טעויות אנוש.

כיצד השימוש בכלי ChatOps מגביר את השקיפות והאחריות של צוותי התגובה והאנליסטים ב-SOC?

בעידן המודרני שבו איומי הסייבר גדלים מדי יום הן בכמות והן ברמת התחכום, ארגונים מחפשים אחר הפתרון המושלם בהתמודדות יעילה עם האיומים הללו. בשנה האחרונה ניתן לומר שיש גל של מומנטום סביב השימוש בכלי ChatOps בתחום הגנת הסייבר. היכולת לשוח עם אנליסטים אחרים, למנף Chatbots לביצוע והרצת פקודות אוטומטיות, להריץ תהליכים אוטומטיים, ולרכז את כל השיחות, רישום, תיעוד וניהול האירוע , וכל זה מפלטפורמה אחת בלבד, מאפשרת ל-SOC להפחית באופן דרסטי את זמני התגובה לאירוע, תוך הגברת האיכות הכוללת ודיוק תהליך התחקור הדיגיטלי של האירוע.

לפני השימוש ב-ChatOps, אנליסטים נמנעו למשתף פעולה בנושא ניהול ותגובה לאירועי אבטחת מידע בגלל התהליך המייגע שנדרש לטובת העניין. שיתוף המידע בין האנליסטים היה מתבצע עד כה באמצעות הדוא"ל או מערכת ticketing, מה שיצר תהליכי עבודה לא יעילים של שליחת נתונים והחלפת נתונים בצורה מסורבלת, ולא יעילה. יתרה מכך, תהליך המעקב אחר ניהול ותגובה לאירועי אבטחת מידע (ישנים ועתידיים) היה מתבצע לעתים קרובות באמצעות נייר (נהלים כתובים). כמו כן, ניסיונות של בדיקה רטרוספקטיבית של בעלות ואחריות על אירועים קודמים היו ניסיונות כושלים וחסרי תועלת ב-SOC.

היעדר שיתוף הפעולה והמידע בין הצוותים השונים הובילו למספר בעיות כגון:

היעדר שיפור מיומנויות וכשירות מקצועית של האנליסטים: היות והארגון חשב שזה יהיה מהיר יותר וחסכוני יותר לטפל באירועי סייבר לפי הגדרת התפקיד וחלוקת המשימות (silos), אנליסטים לא שיתפו מידע, ידע, ניסיון ולא עבדו במשותף לצורך לימוד ושיפור המיומנויות והכשירות המקצועית. כל אחד עבד לבדו, ולא היה שיתוף פעולה לצורך שיפור היכולת של הארגון לטפל באירוע בצורה מרורכזת.

היעדר תהליכי תחקור דיגיטלי אופטימליים: לכל אנליסט ב-SOC הייתה רשימת תיוג (checklist) של מה לעשות בכל יום (או בכל אירוע), איזה מערכות לבדוק, באיזה מערכות להריץ פקודות וכדומה. היות ותהליך התחקור של האירוע בוצע באופן מבודד ולא היה מוזן למאגר מידע מודיעיני מרכזי לניהול ידע, היה קורה מצב שבו, אנליסטים שונים, היו מטפלים באותן סוגי אירועים, בדרכים שונות, ללא שום יכולת של אופטימיזציה, הפקת לקחים וניסיונות לשפר את זמני התגובה או הדיוק של התחקור אירוע.

היעדר מיפוי אחריות לטיפול באירוע: בעוד שנתיב הביקורת ותהליך ניטור משתמשים קיימים עבור משימות סטנדרטיות של תגובה לאירועי אבטחה שונים, זהו מרכיב חסר בהתייחס לתהליך ניהול וטיפול באירוע. בהיעדר מערכת מרכזית של תהליך הטיפול באירוע, קשה לחפש ולבדוק לאחור מי טיפל במה, ישנו חוסר בגרנולאריות מבחינת היכולות לבצע שאילתות על אירועי בעבר. עם ריבוי מערכות ניטור ואבטחה שונות, ועוד מגוון רחב של מערכות נוספות שמעורבות בתהליך התחקור וטיפול באירוע, כגון מסרים מיידיים, דוא"ל, ticketing – ועוד, תהליך החיפוש וקורלציה בין אירועים שונים הינו ארוך ומייגע, ולפעמים חסר תכלית.

חסרונות אלו, הובילו למצב שבו היכולת של ה-SOC לטפל בצורה יעילה באירועי אבטחת מידע הייתה ירודה, והסיכון העסקי גדל כתוצאה מאירועי הסייבר גדל באופן משמעותי.

ה-ChatOps – אור בקצה המנהרה

השימוש במערכות וכלי ChatOps מאפשרים לגשר על הפערים הללו בצורה יעילה ומדויקת יותר. כאשר הצוותים השונים (בקרים, אנליסטים, מהנדסי מערכת, תגובה וכו') מנהלים את האירוע מקונסול אחד מרכזי, כל שיחה, פעולה או פקודה שמריצים הינה גלויה לכל הצוותים שמעורבים בתהליך. זה מספק שקיפות מלאה לכלל הפעילויות שבוצעו במהלך התחקור אירוע, בין אם מדובר בגורמים בתוך הארגון (הנהלה, בקרים, אנליסטים, מהנדסי מערכת, תגובה וכו'), או מחוץ לארגון (בעלי מניות, שותפים עסקיים, לקוחות וכו'). כעת, קל יותר גם לעקוב אחר הבעלות על הטיפול בכל אירוע (מי אחראי על הטיפול בכל אירוע ואירוע), תוך אפשרות להגדרת מדדים למדידת האפקטיביות של הטיפול באירוע (זמני תגובה, זמן טיפול וסגירת האירוע, מידת הנזק שנגרמה כתוצאה מהאירוע ועוד).

השימוש בכלי ChatOps כולל בין היתר את היתרונות הבאים:

אנליסטים לומדים אחד מהשני: לא סתם אומרים: "טובי השניים מן האחד". השימוש בכלי ChatOps מאפשר נראות של כל פעולות האנליסטים (כולל הערות ושיחות שמתבצעות תוך כדי הטיפול באירוע) בקונסול אחד מרכזי, מבלי לפגוע ביעילות הטיפול באירוע. לפיכך, אנליסטים יכולים לשתף כוחות, ידע וניסיון בטיפול ותחקור אירועי אבטחת מידע באמצעות סינרגיה מושלמת מבין כל הגורמים. ע"י שיתוף מידע, כל חברי הצוות (אפילו אלו שמחוסרי ידע או ניסיון) יכולים לתרום את חלקם ואף ללמוד ולחזק את הכשירות המקצועית שלהם בכך שילמדו מתהליך הפקת הלקחים באירועים.

תהליכי תגובה מהירים ויעילים יותר: בנוסף ליתרון הטמון בתהליך למידה אנליטית פרואקטיבית, השימוש בכלי ChatOps מסייע גם ביצירת מאגר ידע מרכזי של מגוון פעולות, פקודות ושיחות (ידע) של אנליסטים ושאר הצוותים שמעורבים בתהליך תחקור האירוע. מסד נתונים זה מבטיח כי הצוותים השונים ב-SOC, יוכלו מעתה לקצר את זמן התגובה והטיפול באירוע (כל צוות תחת האחריות שלו), ובכך למזער את מידת הנזק שעלולה לקרות לפעילות העסקית של החברה. כמו כן, הידע והניסיון שנצבר לאורך השנים נשמר באמצעות מאגר מרכזי אשר נמצא בארגון. יתר על כן, באמצעות שימוש באלגוריתמים ולמידה של שפת מכונה המופעלים על מסד הנתונים שנצבר בארגון, יכול להביא לתובנות שימושיות עבור הצוותים השונים בארגון (בקרים, אנליסטים, מהנדסי מערכת, תגובה וכו') מבחינת היכולת טיפול ותגובה לאירועי הסייבר (למשל, תבניות חוזרות ונישנות של מתקפות סייבר על מערכות הארגון, נקודות חולשה ברשת שתמיד מתקיפים אותנו דרכם, ועוד). באמצעות השימוש בפלטפורמה יחידה – ניתן לייצר בסיס ידע נרחב ותובנות אשר יאפשרו לצוותי התגובה השונים להיות יעילים ומהירים יותר בתהליך התגובה והטיפול באירועי סייבר עתידיים.

הלימה קלה לרגולציה: השימוש בפלטפורמה טובה של ChatOps יכול לסייע בתהליך הלימה לתקינה ורגולציה, ומהווה חלום של כל סוקר או צוות ציות. תיעוד מלא של האירועים והפעילויות שבוצעו במהלך התגובה וטיפול באירוע מאפשרים לצוותים ב-SOC לעמוד בדרישות הנוקשות של תקינה ורגולציה רבות בתחום אבטחת המידע. בכל רגע נתון, ניתן שלוף בקלות כל מידע שרוצים אודות כל אירוע. מנהלי ה-SOC יכולים גם להשתמש בנתונים במערכת על מנת להקצות אחריות ברמת המשמות עבור הצוותים השונים ב-SOC, בהתאם למידת האחריות (בקרים, אנליסטים, מהנדסי מערכות וכדומה). כמו כן, השימוש בפלטפורמה ChatOps מאפשר למנוע עבודת שווא בניסיון לייצר מחדש דרכי פעולה ותגובה לאירועים חוזרים ונשנים, ולטפח סביבת עבודה בעל שקיפות מלאה לכלל הצוותים, ותרבות ארגונית שמעודדת שיתוף מידע וידע ועבודה משותפת.

ללא אכיפה אין אבטחה

פתרון חדשני של חברת CAVIRIN לבדיקת פגיעויות, הקשחות ותאימות למדיניות אבטחת המידע של הארגון תוך הלימה לתקנים ורגולציות רבות בתחום אבטחת המידע יכול למזער לכם את הסיכון למתקפות סייבר עתידיות

הצורך בהגנה על המידע הארגוני והגבלת הגישה אליו היה מאז ומתמיד אחד האתגרים הגדולים ביותר של מחלקת ה-DEVOPS או ה-IT בארגון. בארגונים רבים כיום, מידע ותהליכים עסקיים קריטיים מתבצעים באמצעות שרתים מבוזרים וחשופים להתקפות הן מחוץ לארגון (מחשוב ענן), אך לא פחות מכך לסכנות מתוך הארגון. מחקרים רבים מוכיחים כי עיקר הנזקים שנגרמים לארגון מגיעים מתוך הבית פנימה ונובעים מאי אכיפה של מדיניות אבטחת המידע הארגונית.

בראיון מיוחד עם **יניב מילחוביץ**, סמנכ"ל חברת הייעוץ טיטנס סקיוריטי, הוא מסביר על הסכנות הנובעות מאי אכיפת מדיניות אבטחת המידע בארגון ועל פתרון חדשני מבית CAVIRIN המאפשר לבדוק בזמן אמת את העמידה בדרישות מדיניות אבטחת המידע הארגונית, וכמו כן גם בדרישות תקינה ורגולציות רבות לרבות NIST ,27001 HIPAA, ISO ,GDPR, SOC2 CSF, ועוד.

יניב, מהי הסיטואציה העסקית שהביאה לפיתוחו של פתרון PULSAR מבית CAVIRIN?

על פי דוחות של חברות המחקר וגופים כמו ה-CSI וה-FBI, כ-80% מהחשיפות לפרצות אבטחת מידע מגיעות מתוך הארגון עצמו ולא מבחוץ. ארגונים משקיעים הון עתק בניסיון לחסום את כל הפרצות האפשריות לצורך מניעת מתקפות מבחוץ ואינם מודעים לעובדה שמרבית הבעיות מגיעות מהבית, ע"י הגורם הפנימי. אגב, ברוב המקרים לא מדובר בניסיון לגרום נזק בזדון, אלא פשוט חוסר ידע שגורם לכך שמידע שאמור היה להיות מוגן נחשף לעיני כל, עקב פרצה בשרתים. בחלק מהמקרים מדובר באנשי מערכות המידע או ה-DEVOPS המנסים לפתור בעיות במערכות ה-IT או היישומים הארגוניים תוך כדי כך משנים פרמטרים במערכות עצמן, שמשפיעות לרעה על היבטי אבטחת המידע, וגורמים לכך שהמערכות כבר לא עומדות בדרישות מדיניות אבטחת המידע כפי שנקבעה, מה שחושף את המערכות ואת הארגון לאיומי אבטחת מידע רבים.

כיצד טיטנס סקיוריטי מספקת מענה לאתגרים שציינת?

יניב: כיום קיימים לא מעט פתרונות הקשחה שמוטמעים באתר הלקוח, או בסביבות ענן. אפילו ענקיות ספקי המחשוב ענן, כבר מספקים תשתיות מובנות שכבר מוקשחות עפ"י המלצות Best Practices. ארגונים מחוייבים להטמיע פתרון הקשחה כמענה לדרישות הרגולציה ותקנות בארץ ובחו"ל (כגון הוראת המפקח על הביטוח, על הבנקים, בעולם הרפואי ועוד).

האם תוכל לתת דוגמא ליתרון בשימוש בשירות או במוצר?

יניב: בהחלט. בוא ניקח מצב שבו כמעט בכל ארגון כיום יש יותר מאיש IT או DEVOPS אחד, שמתעסק עם ההקמה של שרתים והקינפוג שלהם. יתכן מצב שבו, אחד מאנשי הצוות, משנה הגדרות (לאו דווקא בכוונת זדון), ובכך מותיר את המערכת חשופה לפגיעויות שונות. באמצעות המוצר, ניתן לסרוק ולאתר כל סטייה ממדיניות אבטחת המידע כפי שנקבעה ע"י הארגון, ונלקוט באמצעים הדרושים לסגור את הפרצות הללו.

דוגמא נוספת, היא המרדף אין סופי לעמוד בדרישות רגולציות רבות. באמצעות המערכת, ניתן להוציא דוחות שונים, להלימה לרגולציות השונות, מה שחוסך זמן רב הן מבחינת עבודת צוותי ה-IT, והן מבחינת עבודתו של הסוקר.

המוצר פועל כקונסול מרכזי , ומשמש ליצירת דוחות על מדדי אבטחה ועמידה בדרישות הרגולטוריות תוך שימוש במסכי תצוגה ברמה הניהולית. המערכת מספקת ללקוחות את הידע הנדרש כדי להבטיח שמערכות המידע של הארגון מאובטחות, מתפקדות באופן אופטימאלי מבחינת רמת אבטחת המידע ותואמות לדרישות כללי מדיניות אבטחת המידע של הארגון, וגם לדרישות רגולטוריות רבות.

חברת טיטנס סקיוריטי, אשר מייצגת את חברת CAVIRIN בישראל בבלעדיות, מציעה ללקוחות שירות ייחודי של בדיקת הקשחות ותאימות לרגולציות ותקינות בעולם אבטחת המידע ופרטיות כגון (GDPR, HIPAA, ISO 27001, SOC2, GLBA, ועוד). השירות כולל קביעת מדיניות הקשחה וניהול תצורה של שרתי החברה (On-Premise או בענן), ובדיקת הקשחות ועמידה בדרישות הרגולציות השונות.

יניב מילחוביץ, סמנכ"ל החברה ומנהל את חטיבת הייעוץ בטיטנס סקיוריטי: "ביצוע פרויקט הקשחת מערכות הינו פועל יוצא של דרישה ועמידה ברגולציות, יחד עם הרצון לשפר את תהליך ההקחשה הנוכחי אשר מתבצע בצורה ידנית ולא מנוהלת. הכלי ייאפשר ייעול העבודה השוטפת בניהול אבטחת המידע. הבחירה בפתרון של CAVIRIN באה בעקבות בחינת יכולת המוצר וכן בשל הניסיון הרב של מומחי טיטנס בתחום ההקשחות".המוצר של CAVIRIN מהווה פתרון ייחודי של בדיקת ניהול תצורה של השרתים, תוך תאימות מלאה לדרישות תקינה ורגולציות רבות. המערכת מאפשרת בדיקת הקשחות, פגיעויות, וסטייה מניהול תצורה של הארגון כפי שנקבע מבוא מועד. עוד כפועל יוצא של המערכת, ניתן ליישם את ההמלצות של הדוח לצורך הקשחת המערכות תוך תאימות מלאה לדרישות רגולציה ותקינה רבות.

האם ישנם גופים שאימצו פתרון זה בארץ וברחבי העולם?

בהחלט. ישנם עשרות ארגונים בארץ ובעולם שאימצו את הפתרון. כך למשל, מדובר בגופים מתחום הפיננסים שהפתרון מאפשר להם מתן מענה רחב יותר לעמידה בדרישות הרגולטוריות. גם חברות שהפעילות שלהם בסביבת מחשוב ענן, משתמשים במערכת על מנת לבחון את רמת אבטחת המידע של השרתים שלהם בענן.

בארץ ובעולם יש לנו לקוחות רבים בתחום הפיננסי, משרדי ממשלה, תעשיית הטלקום, החברות הציבוריות והאשראי, חברות היי-טק ועוד. איני מזכיר שמות כיוון שארגונים אלו אינם מעוניינים לחשוף פרטים אודות מדיניות אבטחת המידע שלהם או האמצעים בהם הם משתמשים.

רק לשם המחשה, אפשר לציין כי הלקוחות אשר משתמשים בשירות שלנו טוענים שזה יצר מהפכה אמיתית ברמת בדיקת אבטחת המידע ומדידת האכיפה של מדיניות אבטחת המידע בארגון, והקטינה של שטח התקיפה מבחינת פגיעויות במערכות בצורה דרמטית.

יתרונות המוצר:

- מוכיח תאימות לדרישות הרגולטוריות
- מרכז את מידע האבטחה כדי להקל על הגישה ועל קבלת החלטות
- הופך נתונים מורכבים למידע בר פעולה
- מספק ניתוח סיכונים רציף

מרבית הלקוחות הטמיעו תהליכי עבודה וכלים שנועדו לבצע רישום אירועים בסביבת מערכות המידע שלהם, אבל הם היו מעוניינים במערכת שתאפשר להם להגדיר קו בסיס שתואמת להמלצות (Best Practices) ונמצא בקו אחד מול דרישות רגולטוריות רבות. כמו כן, המוצר מאפשר ויזואליזציה של מצב התאימות לדרישות החוק של הארגון באמצעות מגוון מדדי תאימות.

המערכת מאפשרת למנהלי מערכות המידע ולאחראי על התאימות לדרישות החוק, רגולציה ותקינה שונות להדגים באופן זמין ומוחשי את מצבה של התאימות באמצעות מיכון והצגת הקשר הקריטי בין כללי מדיניות אבטחת המידע של הארגון, נתונים תפעוליים ותוצאות של רישום אירועים טכניים.

דו"ח שפרסמה חברת האנליסטים Gartner Inc., תומך בהנחה, על פיה ידע הוא נכס חשוב לניהול סיכונים ותאימות לדרישות הרגולטוריות. אחד מהכלים החזקים ביותר לניהול סיכונים בארגון הוא דיווח ברמה גבוהה, אשר מאפשר למנהלים בכירים לקבל החלטות המבוססות על ידע. בנוסף, ממלא הדיווח על סיכונים תפקיד ההולך וגדל בתחום התאימות לדרישות הרגולטוריות.

יתרון נוסף של צוות המומחים שלנו, הינו באספקת שירות על בסיס ידע (Knowledge-based Service Assurance), אשר מספקת ללקוחות את אותו הידע הנדרש כדי להבטיח שמערכות המידע של הארגון מאובטחות, זמינות, מתפקדות באופן אופטימאלי ותואמות לדרישות כללי המדיניות אבטחת המידע של הארגון, וכמו כן לדרישות הרגולציות והתקינה.

תפקידו של ה-CISO בעידן הסייבר

ראיון בלעדי למגזין GLOBAL SECURITY



שנת 2018 כבר החלה, ונראה כי גל מתקפות הסייבר עדיין מרחרח מעלינו, ומאיים על הפעילות העסקית של ארגונים רבים, מכלל המגזרים, גדול כאחד, ונראה כי הטרור הקיברנטי לא פוסח אל אף אחד.

קיימנו ראיון בלעדי עם **לוני יצחק**, מנהל אבטחת המידע והגנת הסייבר בחברת כאל, אשר שיתף אותנו בסוגיות החמות ביותר בתחום אבטחת המידע והגנת הסייבר בכלל, ובאתגרים הניצבים בפני ה-CISO בפרט.

על אף גל איומי הסייבר שפקד עלינו בשנים האחרונות ובעידן הסייבר של היום, עדיין יש לא מעט ארגונים אשר אין להם מנהל אבטחת מידע בכלל, או שקיימת פונקציה כזאת, באופן חלקי בלבד ולא פורמאלי. האם ישנה חשיבות במינוי פורמאלי של CISO בארגון?

בוודאי. בעידן הסייבר של היום, שבו גל מתקפות הסייבר הולך וגובר מצד אחד, ומצד שני הרגולציות ודרישות תקינה שונות נושפות בעורפם של הנהלות הארגונים בכלל המגזרים, ישנה חשיבות עליונה למינוי פורמאלי של CISO בארגון. ה-CISO בארגון מהווה מעין Coacher של הנהלת הארגון מכל הנוגע לתחום אבטחת המידע והגנת הסייבר, ומסייע לו בניהול סיכונים בהיבטים אלו.

מהן היתרונות הנוספים לארגון בכך שימנו תפקיד פורמאלי של CISO?

ה-CISO הינו תפקיד רוחבי בכל הארגון, והוא עובד אל מול כלל המשתמשים, החל מהנהלת הארגון והדירקטוריון, ועד אחרון העובדים. כמובן, הפוקוס והמשקל מתחלק באופן שונה, אבל ה-CISO מהווה ציר מרכזי בכל ארגון. אחד מתפקידו העיקריים של ה-CISO הינו הוספת פן עיקרי וחדש לניהול הסיכונים המסורתי והוא סייבר עסקי – כיצד מתקפת סייבר יכולה להשפיע על תהליכים עסקיים ולוודא בקרות מתאימות לכל תהליך. בנוסף, לעמוד בדרישות תקינה ורגולציות רבות, הן בארץ והן בעולם. מרבית הרגולציות דורשות מינוי פורמאלי של CISO, אשר אמון על כלל מערך אבטחת המידע והגנת הסייבר בארגון. ה-CISO גם מסייע לארגון להשיג הלימה לדרישות תקינה, רגולציה ואף דרישות חוזיות של לקוחות.

לעניות דעתך, למי אתה חושב שה-CISO צריך לדווח בארגון?

ה-CISO חייב לדווח ישירות להנהלה. החשיבות והתרומה של ה-CISO בכל ארגון כיום, הינה חיונית להמשכיות עסקית וניהול סיכונים בתחום אבטחת המידע והגנת הסייבר, ולכן על ה-CISO לדווח ישירות להנהלת הארגון. בצפון אמריקה, ל-CISO יש משקל כבד במבנה הארגוני, והוא מדווח ישירות להנהלת הארגון. בארץ, למעט בפיננסי וביטוח, המצב אינו דומה, ועל מנת לבצע את תפקידו בצורה הטובה ביותר ולביות בעל השפעה בארגון, עליו לדווח ישירות להנהלת הארגון.

כיצד אתה רואה את תפקידו של ה-CISO בארגון? האם הוא צריך להיות טכנולוג או מתודולוג?

השאלה טיפה טריקית, היות וזה הרבה תלוי בסוג הארגון, גודל, מבנה ארגוני, היררכיה, ועוד פרמטרים נוספים. אבל בגדול, על ה-CISO להיות יותר עם אוריינטציה ניהולית ואסטרטגית מאשר טכנולוגית. כפי שציינתי, ה-CISO מהווה מעין Security Coacher להנהלת החברה, והוא מייעץ בכל הקשור לאסטרטגיה ומדיניות אבטחת המידע והגנת הסייבר, שצריכה להיות בהלימה עם האסטרטגיה העסקית של החברה. על ה-CISO להכיר ולהבין היטב את הפעילות העסקית בארגון, כדי לאפשר ולתמוך בעסק, ולא לפגוע בו.

בארגונים טכנולוגיים קטנים, כגון חברות הזנק, נהוג שה-CISO יהיה גם עם אוריינטציה טכנולוגית, היות ובגלל היעדר משאבים, הוא גם הגורם שמתקין ומתפעל את מערך אבטחת המידע מבחינת התשתיות. אבל זה לא נכון לפעול ככה, וכדאי לעשות הפרדה בין הגורם המנחה לבין הגורם המבצע. הפרדה זו היא בריאה לארגון, ובטווח הארוך מביאה ערך מוסף לארגון.

מה לדעתך הידע הנדרש היום מה-CISO?

באחד הכנסים בחו"ל, שמעתי את אחד המרצים על הבמה, שטען שתפקידו של ה-CISO כיום הוא שיווק ומכירות ואני מסכים עם זה בהחלט. עליו להכיר היטב את הפעילות העסקית ולוודא שהאסטרטגיה של אבטחת המידע והגנת הסייבר נמצאת בהלימה עם האסטרטגיה העסקית. ה-CISO חייב לשמור על קשרים טובים על כלל הסגל הניהולי, עם אנשי ה-IT וגם עם המשתמשים בארגון. ה-CISO חייב לשנות את הגישה מלומר: "לא, אי אפשר", ל"אפשר, אבל חייבים לוודא שזה מאובטח על מנת לא לפגוע בפעילות העסקית". חשוב לזכור שאבטחת המידע הוא Business Enabler ולא Business Disabler.

מהן הכישורים הנדרשים היום מה-CISO?

בראש ובראשונה, על ה-CISO להיות בעל כישורים ניהוליים כגון הבנה עסקית, ראייה רוחבית, חשיבה אסטרטגית, יכולת התבטאות בעל פה ובכתב, יכולת עמידה בפני קהל וכמובן גם כושר שכנוע טוב (ולכן ישנם שאומרים שתפקידו של ה-CISO הינו שיווק ומכירות). לארגונים גדולים, בהם ה-CISO מנהל גם צוותי אנשים, נדרשים לו כישורים ניהוליים נוספים כגון ניהול עובדים, יחסי אנוש, ועבודה בצוותים.

ה-CISO יכול להיות גם בעל רקע או ניסיון טכנולוגי, אבל חשוב שלא יאבד את עצמו ביום-יום מתעסק בהתקנה והפעלת מערכות אבטחת מידע, אלא בתכנון ומימוש האסטרטגיה של אבטחת המידע והגנת הסייבר, שחייבת להיות בהלימה עם האסטרטגיה העסקית.

מהם האתגרים העיקריים הניצבים בפני ה-CISO בעידן הסייבר של היום?

ניתן לחלק את האתגרים לשני חלקים עיקריים: אתגרים מתוך הארגון, כגון הטמעת תרבות ארגונית של מודעות כלל העובדים לנושא של אבטחת מידע והגנת הסייבר מצד אחד, אל מול דרישות TTM וחדשנות בעולם הדיגיטלי מצדו השני. ואתגרים מחוץ לארגון, כגון מענה למתאר איומי הסייבר ההולכים וגדלים מצד אחד, אל מול דרישות הרגולטורים והלקוחות מצדו השני. נושא ה-GDPR הינו אחד הנושאים החמים אשר הולך לתפוס מקום מרכזי בחדשות בשנה הקרובה. ארגונים מצאו את עצמם בבהלה ומרדף כנגד השעות בניסיון להביא את הארגון להלימה עם דרישות הרגולציה. ניהול הסיכונים שנובע משרשרת האספקה הינו גם אחד הנושאים המרכזיים שיטריד את הנהלת הארגון. כמו גם, הניסיון להתמודד עם הצורך באבטחת התקני ה-IOT אשר הולכים ותופסים תאוצה בכל ארגון.

תפקידו של ה-CISO בעידן הדיגיטלי של היום, שבו הטכנולוגיות משתנות בהרף עין, הינו אחד מהתפקידים המאתגרים ביותר בארגון.

מהם איומי הסייבר המשמעותיים ביותר שארגונים נאלצו להתמודד איתם במהלך 2017, ומה מיוחד באיומים אלו?

אחד מאיומי הייחוס הבולטים ביותר, ולא רק השנה, אלא גם בשנים האחרונות הינו נוזקת הכופר. לאורך השנתיים האחרונות ראינו מוטציות שונות של נוזקת כופר, אשר גרמה לנזקים של מאות מיליוני דולרים ברחבי העולם. לצד זה, שתי תופעת אומנם לא חדשות, אבל תופסות תאוצה מדי שנה הינם מתקפות מניעת שירות מבוזרות (DDOS) ומתקפות פישינג לסוגיהם (כולל Spear Phishing ו- Whale Phishing). אלו איומי הסייבר המשמעותיים ביותר, אשר ימשיכו להטריד את הנהלות הארגונים גם בשנים הבאות.

מהי התחזית שלך למפת איומי הסייבר לשנת 2018?

ובכן, נוזקות הכופר (לסוגיהן) ימשיכו להטריד אותנו גם בשנים הבאות. כנ"ל מתקפות DDOS ומתקפות פישינג. בנוסף, אחד הטרנדים החמים הינו האיום שנובע משרשרת האספקה, כלומר עבודה עם גורמים צד ג'. נוזקות ומתקפות APT על התקני IOT הינו גם אחד האיומים המאתגרים לשנים הבאות. אחת המגמות הנוספות שתופסת תאוצה הינה "מתקפות וכלים כשירות" (Crime-as-a-Service). מדובר בתופעה שבה ניתן יהיה להזמין מתקפות ו"פריצות" מוכנות ומתוזמנות ברשת השחורה.

מהי הדרך הטובה ביותר להימנע ממתקפות סייבר?

ובכן, אין Silver Bullet כשמדובר בהגנה הרמטית מפני מתקפות סייבר, ולחשוב אחרת זה יהיה נאיבי מצידו של כל ארגון. כיום. התפיסה השתנתה, והארגונים חייבים להבין שזאת לא שאלה של האם, אלא מתי או האם זה כבר קרה לי. על הארגון לגבש אסטרטגיה בתחום אבטחת המידע והגנת הסייבר, לאמץ מסגרת לניהול תחום זה, לבנות תוכנית עבודה ולהוציא אותה לפועל.

הארגון חייב להבין מהם איומי הייחוס שרלוונטיים לגביו, ולהטמיע מערך הגנה הולם שימנע או לפחות ימזער את מידת ההשפעה של מתקפות הסייבר על הפעילות של הארגון. המערך חייב להיות בנוי ממספר אלמנטים כגון: אנשים מוכשרים, תהליכי עבודה יעילים, ובקרות הגנה הולמות. מימוש אוטומציה בתהליך ניהול ותגובה לאירועי אבטחת מידע יכול לעשות את כל ההבדל מכישלון מוחץ, להתאוששות מהירה מכל אירוע סייבר.

חשוב גם לשמור על כשירות מקצועית של הצוותים הרלוונטיים, ולתרגל אותם מדי פעם. זה יסייע בשמירה על עירנות.

במידה וארגון מותקף, כיצד ניתן להתאושש ביעילות ממתקפת סייבר?

זה תלוי כמובן בסוג התקיפה, הווקטור, מטרת התקיפה, סוג התוקף, ועוד גורמים נוספים. אבל בעת אירוע סייבר, חשוב שיהיה מערך ניטור וזיהוי הוליסטי אשר יכלול אמצעי זיהוי, איסוף לוגים וקורלציה בין לוגים של מערכות שונות, כגון מערכת SIEM, אשר תסייע ל-CISO לקבל תמונת מצב אמיתית אודות התקיפה.

כמו כן, אחד היתרונות הינו שימוש באוטומציה. הוכח כי שימוש באוטומציה בתחום זיהוי ותגובה לאירועי סייבר, הוכיח את עצמו מבחינת ROI.

הספקים נמצאים כיום במעין מרדף אין-סופי למצוא את הפתרון הפלא הבא בעולם הגנת הסייבר. אילו טכנולוגיות או מגמות לדעתך יעניינו את ה-CISO במהלך 2018?

לוני: בהיבטים הטכנולוגיים, העולם הולך יותר לכיוון של אוטומציה ותזמון מערכות (Orchestration), פתרונות שמבוססים על AI ו-Machine Learning, וניסיונות למצוא את הדבר הבא מבחינת המערכות ההגנה האולטימטיביות.

בהיבטים הניהוליים, נושא הרגולציה האירופאית תמשיך לעשות גלים ולהעסיק את הנהלת הארגונים, וכמו כן, גם נושא ניהול הסיכונים של שרשרת האספקה.

האם ניתן לומר שחלה עלייה במודעות הנהלות הארגונים בנושא אבטחת המידע והגנת הסייבר?

בהחלט כן. וזה לצערי הרב תודות לגל מתקפות הסייבר אשר פקד על ארגונים בארץ ובחו"ל בשנים האחרונות. כיום, הנהלות הארגונים מודעים יותר לחשיבותו של תחום אבטחת המידע והגנת הסייבר, וישנם ניסיונות רבים להוציא לשוק מסגרות ותקנים שמספקים המלצות והנחיות כיצד להתגונן מפני מתקפות הסייבר.

ולסיום, מה דעתך על פעילות האיגוד העולמי לאבטחת מידע (ISSA), ובייחוד על הפעילות של הציאפטר הישראלי?

נחשפתי לפעילות הזאת לפני כחצי שנה, ואני חייב לציין שאני מרוצה מעצם ההתקדמות של הציאפטר הישראלי, ומהעשייה ותרומתו של הציאפטר לשוק המקומי.

השתתפתי במספר מפגשים, שהיו מאוד מקצועיים ומרתקים, ומצפה בכיליון עיניים לפעילות ענפה גם בהמשך השנה.

תפקידו של ה-CISO במניעת אירועי סייבר

בעידן הסייבר, שבו כמות אירועי הסייבר ממשיך לגדול הן מבחינת הכמות והן מבחינת רמת התחכום של התקיפה, ה-CISO מרגיש כמו חיה פצועה מול כיתת יורים. השאלה שנשאלת היא לא האם יתרחש אירוע סייבר בארגון, אלא מתי זה יתרחש, והאם הארגון מוכן ובעל יכולת לזהות ולהגיב בזמן אמת.



מאת: **טוני וולושקו**,
מנהל אבטחת המידע
של חברת NEXAR



בעוד שמשרת ה-CISO היא אחת המשרות הנחשקות בתעשייה, לפעמים מדובר בתפקיד כפוי טובה.

למרבה הצער, תפקידו של ה-CISO הינו אחד מהתפקידים המהותיים ובעלי אחריות כבדה (אפילו אחריות אישית במדינות מסוימות בעולם, בייחוד בצפון אמריקה) במקרה של תקרית סייבר שבה מידע רגיש זולג לידיים הלא נכונות.

ישנם מחקרים שמראים תמונה עגומה, שבה במרבית הארגונים, הגורם הראשון שמואשם בגרימת תקרית הסייבר הינו ה-CISO (כ-40%), כאשר מיד אחריו ניצב המנכ"ל (כ-35%).

ובכן, ה-CISO יכול ואף חייב לנקוט בצעדים הנכונים ומבוא מועד, על מנת למעזר את האפשרות שהחברה תיפול קורבן לתקריות סייבר מביכות. ואם תקריות הסייבר אכן קורות, וה-CISO נקט בכל הצעדים הנדרשים לצורך מזעור הסיכון, אז הוא יכול לעמוד עם ראש זקוף בפני הנהלת הארגון ושאר הגורמים הרלוונטיים (כגון בעלי המניות, חברי הדירקטוריון, רגולטורים וכו').

לפניכם מספר שיטות וצעדים, שכל CISO חייב לפעול לפיהם, כדי להימנע מלהפוך שעיר לעזעזל, ואף להפוך את הקערה עלפיה, ולהצליח לשפר בצורה משמעותית את רמת הבשלות של הארגון מבחינת אבטחת מידע, ובכך לתרום לחיזוק השרידות הקיברנטית (Cyber Resilience) והפעילות העסקית של הארגון.

מהו תפקידו של ה-CISO?

ובכן, מהו תפקידו של ה-CISO? בגלל שתפקידו של ה-CISO קיים רק עשור או שניים, לא מעט אנשים עדיין לא יודעים מה נדרש מתפקידו של ה-CISO, עובדה מצערת שלא ממש תורמת ל-CISO במקרה של קרות אירוע סייבר, שאז קל מאוד להאשים אותו בכך.

ה-CISO (ר"ת של Chief Information Security Officer) מהווה מעין קצין אבטחת מידע ראשי של הארגון, והוא מוגדר כגורם המנהל הבכיר שאחראי על ביצוע ופיקוח האסטרטגיה ומערך הגנת הסייבר בארגון.

חלק מהאחריות של תפקידו של ה-CISO מכיל את הפעילויות הבאות:

- גיוס צוותי אבטחת מידע
- ביצוע קמפיינים להגברת המודעות בנושא אבטחת מידע וסייבר
- אפיון, גיבוש, כתיבה ואכיפת מדיניות ונהלי אבטחת מידע וסייבר בארגון
- תכנון שרידות קיברנטית ורציפות תפעולית
- ניטור מערך ה-IT והייצור לזיהוי ומניעת פגיעויות (ניהול פגועיות)
- לוודא שמירה על פרטיות המידע
- קביעת מדדים ומדידת האפקטיביות של הבקרות ומערך הגנת הסייבר
- בחינת ורכישת מוצרי אבטחת מידע (שתואמים לדרישות העסקיות של הארגון)
- ניהול ותגובה לאירועי סייבר
- לוודא הטמעת תהליכי פיתוח מאובטח
- לנהל סיכונים בשרשרת האספקה של הארגון
- לוודא הלימה לדרישות חוקיות, תקנות ורגולציות ישימות לארגון

ככל שסביבות ה-IT והיישומים השונים נהיים מורכבים יותר מפעם לפעם, האחריות של ה-CISO הולכת ומתרחבת בהתאם. לנסות לטפל בכלל המשימות הללו ולתת מענה הולם, ובזמן אמת נראה כמשימה בלתי אפשרית, ולעתים גם לא זוכים להערכה ראויה.

גופי מחקר שונים מראים כי כהונת CISO ממוצעת בארגון הינה כ-18 חודש. למרות שמדובר בתפקיד יוקרתי, שמקבל תגמול כספי הולם, מדובר באחד התפקידים שממלא המשרה נמצא על קוצים ובלחץ רוב הזמן, תפקיד שבו פיטורים ועזיבה הם נפוצים יותר משאר בעלי התפקידים ב-IT.

כיצד ה-CISO יכול להגין על החברה ולא פחות חשוב, על עצמו?

שקיפות ודיווח רציף

אם מתגלה פגיעות בתשתית ה-IT של ארגון, אך המידע הרגיש מוגן מפני גישה לא מורשית, האם ה-CISO יפוטר? שקיפות תפעולית היא המפתח להצלחה בתפקיד. פירוש הדבר הוא שעל ה-CISO לוודא דיווח מדויק ועקבי של נקודות התורפה (חשיפות), כל אי-התאמה לדרישות אבטחה או רגולציה שמתגלה בתשתיות המחשוב של הארגון, וכמובן על תקריות אבטחת מידע וסייבר – ולא משנה מה מידת הנזק או רמת הסיווג של האירוע. תזכרו, ששקיפות תפעולית היא שם המשחק.

כהמלצה, גישה זו של שמירה על שקיפות מול הלקוחות יכולה לסייע במניעה, כמו כן בגילוי, זיהוי וטיפול (תחקור) של תקריות אבטחת מידע כשיקרו.

היה מקרה אחד בולט במיוחד, שבו ה-CISO הבטיח אלפי דולרים לבודק מומחה (האקר אתי) שגילה פגיעות באחד השרתים של החברה, אך ה-CISO לא דיווח על כך בזמן למנכ"ל. ה-CISO גם התעלם מהפניות החוזרות ונשנות של הבודק, וכמובן גם לא שילם את כספי הפרס כפי שהובטח. למרבה המזל, התקרית נתגלתה ע"י מנכ"ל החברה, שפיטר באופן מיידי את ה-CISO עקב רשלנות בתפקיד (אי שיתוף המידע בזמן) וכמובן שילם לבודק שהיה אחראי לגילוי הפגיעות.

חשוב לגייס את הצוות הנכון

קל יותר לומר מאשר לבצע, אבל על ה-CISO לנסות לגייס את אנשי המקצוע המתאימים ביותר לביצוע התפקידים שנדרשים בארגון, ולא משנה מה הרקע שלהם. ידוע, בייחוד בתחום ה-IT והסייבר, הם אוטודידקטיים ולמרביתם אין תארים פורמאליים. בחברות גדולות בארה"ב, ההנהלה אוהבת לקרוא לאנשים הללו "צווארון לבן", אשר שמים יותר דגש על כישרון, מיומנויות וכישורים על פני תארים וקריירות קודמות.

מדובר בשינוי מהותי בתהליך הגיוס וקליטת עובדים חדשים, וה-CISO יכול לשים יותר דגש על מציאת האדם בעל הכישורים והפוטנציאל הטוב ביותר, ופחות להתמקד בתארים חסרי תועלת. ה-CISO יכול לקיים מבחנים שונים לצורך בחינת הכשירות המקצועית של המועמדים, על מנת להעריך את היכולת שלהם מבחינת קבלת החלטות, היכולת ללמוד לבד או בצוות, ואת הכשירות המקצועית לטיפול באירועי אבטחת מידע וסייבר.

לקבל גיבוי מהנהלת החברה

חשוב מאוד לוודא שהנהלת הארגון שומעת בקולו של ה-CISO, ומתייעצים איתו בנושאים שקשורים לאסטרטגיה וניהול מערך אבטחת המידע בארגון, שתואם לאסטרטגיה ולמטרות העסקיות של הארגון. בשנים האחרונות, ה-CISO הגיע לרמה של חשיבות אסטרטגית בארגונים רבים, רמה השווה לזו של המנמ"ר (CIO). משמעות הדבר היא של-CISO אכן מגיע מקום בזכות ליד השולחן בחדר המנהלים.

אחת המגמות הנפוצות ביותר מבחינת ההיררכיה הארגונית, היא שה-CISO מדווח ישירות למנכ"ל החברה, מגמה שיכולה בהחלט לסייע לקשר ביניהם. אומנם ל-CISO יש השפעה או שליטה מועטה על קביעת המבנה הארגוני, חשוב בכל זאת שקולו ישמע על ידי הנהלת החברה, היות והנושא של שרידות קיברנטית, רציפות תפעולית ושמירת המוניטין של החברה נשענות אכן על האסטרטגיה של אבטחת המידע בארגון.

שימוש בפתרונות ובכלים הנכונים

קביעת ארכיטקטורה שמבוססת על פתרונות אבטחה סטנדרטיים, הינו מודל מיושן, שאינו עומד באמות המידה אל מול גל איומי הסייבר ההולך וגובר.

חברת המחקר פורסטר, ציינה באחד הדוחות האחרונים שלה כי "גישת אבטחת המידע המבוססת על הגנה היקפית הינו מודל מיושן ולא יעיל. מומחי אבטחת מידע ממליצים לנקוט גישה חדשנית שממוקדת על הגנת נתונים באשר הם יהיו (בענן, באתר הלקוח, במובייל וכו') ובכך לוודא שאבטחת המידע תיסע עם הנתונים עצמם – ובכך לבטיח הגנה נאותה על המידע ופרטיות המידע.

בשל הנתונים הרגישים בעלי הערך הרב שיש להם, ארגונים פיננסיים פגיעים ומהווים מטרה שכיחה יותר בקרב קבוצות האקרים, ובייחוד אל מול האויב שבפנים (גורם פנימי). על ה-CISO לאמץ מודל הגנה בשכבות, על מנת למזער את הסיכון למימוש איומים ותקריות אבטחת מידע וסייבר. על ה-CISO לוודא שכלל הבקרות בכל שכבה יעילות ומתפקדות כראוי, תוך מדידת מתמדת של האפקטיביות של הבקרות לוודא רציפות תפעולית.

חינוך משתמשים והגברת המודעות בנושא אבטחת מידע וסייבר

אחת מהמשימות החשובות של ה-CISO בארגון הינה להפוך את העובדים להיות מודעים יותר ויותר לאיומים השונים בתחום אבטחת מידע וסייבר. עליו לגבש קמפיין להגברת המודעות בנושא אבטחת מידע, ולוודא שכלל העובדים הרלוונטיים עוברים הכשרות והדרכות לצורך שמירה על הכשירות המקצועית שלהם. היכולות של המערכות ניטור ושירותי מודיעין הסייבר לא יבואו לידי ביטוי בצורה אופטימאלית, אם ה-CISO לא ישתף את המידע הזה עם כלל המשתתפים.

הגברת המודעות של העובדים לאיומי אבטחת מידע וסייבר הינו נדבך חשוב מאוד בחיזוק שרשרת האבטחה של הארגון.

בידוד ותגובה מיידית לתקריות אבטחה

חשוב לזכור, שגם עם בנינו את מערך אבטחת המידע והגנת הסייבר המושלם ביותר, תקריות סייבר יכולות לקרות, היות וההאקרים נהיים יותר אגרסיביים ומתוחכמים בשיטות התקיפה שלהם. מה שה-CISO יכול לעשות, הוא לנסות לצמצם את זמני התגובה לאירועי הסייבר ולמנוע התעכבות מיותרת בשל הכנה לא נאותה מבוא מועד. הכנה יעילה יעשה את כל ההבדל בין כישלון ופגיעה בפעילות העסקית, להצלחה.

השקעה בכלים הנכונים, ובכח האדם המיומן המתאים, יכול לסייע ל-CISO להגיב בצורה מהירה (קרוב ככל האפשר לזמן אמת), ובכך למזער את הסיכון למימוש האיום, או לפחות לנסות לצמצם את מידת הנזק האפשרית כתוצאה מהאירוע סייבר.

חשוב לזכור, שה-CISO הינו אחד מהמשאבים הקריטיים ביותר בארגון, אך לעתים קרובות הם מוצאים את עצמם שעירי לעזעזל במקרה של תקריות סייבר בהם דלף מידע רגיש מחוץ לגבולות הארגון. עם זאת, אם ה-CISO החכים לאמץ את ההמלצות שתיארתי כאן, הוא יכול לשפר את רמת השרידות של הארגון במקרה של אירועי סייבר, ולהגן על עצמו מפני נזק אישי.

ה-CISO שפעיל בצורה פרואקטיבית, ופועל בנמרצות לחזק את מערך ההגנה של הארגון, יצליח למזער ואף למנוע במקרים מסוימים, את הסיכון למימוש של גל איומי הסייבר שעתידים לפקוד על הארגון.

> חשוב מאוד לוודא שהנהלת הארגון שומעת בקולו של ה-CISO, ומתייעצים איתו בנושאים שקשורים לאסטרטגיה וניהול מערך אבטחת המידע בארגון.



TSG Titans Security Group

הביטחון שלך, זו העבודה שלנו.

טייטנס סקיוריטי, האוטוריטה בתחום אבטחת המידע, מציעה קשת של שירותים מתקדמים בתחום אבטחת המידע למוסדות וארגונים.

החל בייעוץ אובייקטיבי
עם מומחים בעלי שם עולמי, וכלה בליווי
פרויקטים בתחום אבטחת מידע.

הגדרת אסטרטגיה
ותפיסת ממשל אבטחת מידע בארגון

הכנת הארגון
לעמידה בדרישות רגולציה שונות

אפיון דרישות מערכת,
כתיבה וליווי במכרזים

בחירת טכנולוגיה
המתאימה ביותר לארגון בתהליך RFP מסודר ושיטתי

ניהול פרויקטים
אבטחת מידע מורכבים

לתיאום פגישה וקבלת פרטים נוספים:
טלפון: 077-5150340 | info@titans2.com

תמונתה של מונה ליזה

Out

מפות תקיפות עולמיות

In

במרבית המרכזים לניהול אירועי אבטחת מידע (SOC) צוות האנליסטים קישטו את חלל החדר במסכי פלזמה ענקיים, שעליהם מוצגות מתקפות עולמיות בתצורות שונות.

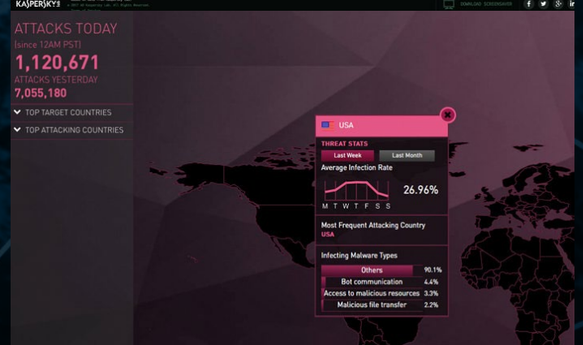
ספקים שונים מספקים שירותי מפות תקיפה מקוונות, בהן מוצגות תקיפות סייבר ברחבי העולם, כולל פרמטרים אודות מהות התקיפה, יעד, מקור, ועוד פרמטרים רבים נוספים. בעוד שמטרתן של המפות הללו הינה למשוך את עיניהם של המבקרים בחדרי ה-SOC, ניתן גם לעשות בהן שימוש מושכל לטובת תחקור אירועי סייבר ומגמות בעולם.











אחת מהטעויות הנפוצות היא ההנחה שהמידע שמוצג הינו בזמן אמת. אז זהו שלא. מדובר בהקלטה של תעבורת מידע ומתקפות שנאספו לצורכי תחקור, וכעת מוצגים בתצורה שנראית יפה לעין.

אך למפות הללו יש גם לא מעט יתרונות מלבד היופי שלהן. בעת ביקורים ב-SOC, הן של ההנהלה והן של משקיעים או אורחים שונים, מפות אלו מספקות תצוגה ויזואלית מרשימה.

בנוסף, על סמך שיחות עם מנהלי SOC רבים, לעתים נעשית פעילות העשרה של ביקורים תלמידים מבתי ספר שונים שלומדים במגמות סייבר, וזה מעודד אותם ללמוד את התחום, היות וזה נראה כמו בסרטים, מאוד מרתק, מפת תקיפה עולמית של אירועי סייבר.

על סמך התצוגה של המפות הללו, ניתן לקיים דיונים ולנתח מקרים של סוגי תקיפות שונים, מהן מקורות התקיפה, מהן היעדים הכי מבוקשים, מהן שיטות התקיפה וסוכני האיום.

אנליסטים שונים ב-SOC,אשר מספקים שירותים מנוהלים (MSSP) נעזרים גם במפות הללו על מנת להציג ויזואלית ללקוחות שלהם את מהות הפעילות של הניטור וחשיבות העבודה של ה-SOC. שוב, חשוב לזכור שהערך המוסף בתצוגה הויזואלית של המפות הללו אינו בתוכן המידע שמוצג, אלא בשיחות וניתוח המקרים שלאחר מכן, בהן צוותי התגובה והאנליסטים יכולים להיעזר לצורך תחקור אירועים והפקת לקחים.

לפניכם ריכזנו מספר מפות תקיפה עולמיות, מהשכיחות ביותר.

מפת תקיפות סייבר עולמיות של חברת NORSE

ככל הנראה המפה הכי פופולארית של הצגת תקיפות סייבר עולמיות. החברה מציגה מפת איומים שמבוססת על מגוון עצום של נתונים וכריית מידע שנאסף באמצעות תשתיות מלכודות דבש (Honeypot) שהחברה פרסה ברחבי הרשת.

מה שיפה במפה זו, זאת האפשרות להוסיף את הלוגו של הארגון עצמו שעושה שימוש במפה, כך שזה יראה שמדובר בכלי שפותח בתוך ה-SOC עצמו, וזה נראה מרשים ויזואלית.

מפת תקיפות סייבר עולמיות של חברת קספרסקי

אחת המפות היפות ביותר מבחינה ויזואלית, הינה מפת האיומים של קספרסקי. למפה ישנה גם אפשרות אינטראקטיבית של הזזת המפה, וביצוע תקריב (zoom) על נתונים ספציפיים.

הנתונים שמוצגים על מפה זו נלקחו ממגוון מקורות מידע כגון מוצרי אנטי-וירוס וסינון תוכן ברמת תחנות עבודה, שרתי דוא"ל, ושרתי Web, וגם של סריקות יזומות אחרות ברשתות שונות.

מפת תקיפות סייבר עולמיות של חברת FORTINET

המפה דומה לזו של חברת NORSE, ומציגה נתונים של תקיפות שמבוססים על תעבורה מוקלטת של תקשורת נתונים שבוצע לטובת ניתוח ותחקור אירועים.

בתחתית המסך, ישנן סטטיסטיקות שונות שרצות אודות התקיפות. כמו כן, עפ"י תיעוד, ללקוחות החברה ישנה אפשרות לבנות מפת איומים ותקיפות ייחודית משלהם.

מפת תקיפות סייבר עולמיות של חברת CHECKPOINT

מדובר במפה אקטיבית, שמציגה נתונים היסטוריים שמתאפסים בכל יממה בשעה 00:00 בלילה. המפה היא יותר יפה ויזואלית מאשר של חברת NORSE, אבל הפונקציונאליות דומה.

בנוסף לצפייה בתצוגת הנתונים במפה, ניתן לבצע חיפוש ולצפות בהיסטוריה של תקיפות עפ"י חתכים שונים: מקור תקיפה, יעד תקיפה, שיטות תקיפה ועוד. מידע זה שימושי מאוד לבניית מצגות להנהלה, למשקיעים, ללקוחות, ולצורכי למידה, מחקר, וניתוח מגמות.

מפת תקיפות סייבר עולמיות של חברת FireEye

מפה זו שומרת על פשטות ויזואלית, ומציגה נתונים בחתכים של מגזרים, ומיהם המדינות המובילות מבחינת התקיפות (מקור התקיפה). הנתונים שמוצגים מתבססים על ניתוח של מתקפות אמיתיות, שנותחו ע"י האנליסטים של החברה, ומוצגים על המפה מבחינה ויזואלית.

מפת תקיפות סייבר עולמיות של חברת ARBOR NETWORKS

מדובר במפה אינטראקטיבית שנוצרה בשיתוף עם Google Ideas. המפה שמציגה בעיקר תמונת מצב על מתקפות מניעת שירות מבוזרות (DDOS) מקבלת נתונים מתוך המערכת שירותי מודיעין סייבר של Arbor ATLAS. המידע שמוצג מתבסס על כריית נתונים מתוך 300 ספקיות אינטרנט ברחבי העולם, ותעבורה גלובאלית של למעלה מ-130 טרה-בייט.

המפה מציגה מגוון מתקפות DDOS, ומאפשרת לבצע פילטור עפ"י סוגי תקיפה וגודל התקיפה.

מפת תקיפות סייבר עולמיות של חברת TREND MICRO

מדובר במפה שמציגה נתונים ויזואליים אודות תקיפות של רשתות בוטים (Botnets) עם מידע אודות מיקומם של שרתי C&C (Command & Control) ברחבי העולם. המפה מציגה היסטוריית נתונים של עד 14 יום אחורה.

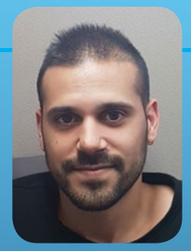
מפת תקיפות סייבר עולמיות של חברת AKAMAI

אומנם לא מדובר במפה שמטרתה להציג תמונת מצב של מתקפות סייבר עולמיות, אבל מעבר להצגת נתונים אודות תעבורת הרשת באינטרנט, המפה מספקת גם מידע שימושי אודות מתקפות מסוימות (בעיקר DDOSS).

ניתן לראות באמצעות המפה באיזה אזורים בעולם ישנה תעבורת רשת גדולה מאוד (חריגה), וגם איזה אזורים אכן נפלו קורבנות למתקפות סייבר (DDOS). לטענת החברה, המידע שמוצג הינו מידע חיי, שמייצג זמן אמת.

אסטרטגיות לניהול והפעלת SOC

שנת 2018 כבר החלה, ונראה כי גל מתקפות הסייבר עדיין מרחרח מעלינו, ומאיים על הפעילות העסקית של ארגונים רבים, מכלל המגזרים, גדול כאחד. קיימנו ראיון בלעדי עם שני מנהלי SOC, אשר שיתפו אותנו בסוגיות החמות ביותר בתחום אבטחת המידע והגנת הסייבר.



אבירן אוחנה
בנק הפועלים



אוראל ביתן
מנהל SOC בסלקום

במחלקת משאבי אנוש כך גם קיים הצורך שיהיה מערך שיודע להכיל ולטפל באירועי תקיפה בזמן אמת על הארגון.

מהם הטעויות שכיחות ביותר שניתן לעשות בהטמעה וניהול SOC בארגון?

אבירן: אפיון לא נכון של מערכות הניהול ב-SOC בהתאם לצרכי הארגון, מיפוי התהליכים הקריטיים לטובת ביצוע ניטור יעיל, תקופת הכשרה קצרה ולא מספיק מקיפה לאנליסטים, הגדרה לא נכונה של תחומי אחריות ה- SOC, בניית נהלים שאינם תואמים את מדיניות הארגון, אינטראקציה לקויה מול הגורמים המנהליים והתפעוליים.

אוראל: הטעות הנפוצה ביותר היא חוסר סדר וארגון. קל מאוד להתבלבל בחלוקת האחריות ובסדר ההטמעה, מנהל חייב לדעת להגדיר לכל צוות במערך ה-SOC את גבולות הגזרה שלו ושהוא יהיה המוביל באותו התוכן. בחירת אנשים מקצועיים מספיק שיודעים איך למנף את יכולת ההגנה על הארגון לדעתי- צורת הגיוס הכי יעילה של עובדים היא ע"י Challenge ובדיקת צורת החשיבה וההתמודדות של המועמד עם אתגרים ולא פתרון סופי.

האם החשיבות של ה-SOC עלתה עם השנים או ירדה?

אבירן: אין ספק שהחשיבות עלתה, ובאופן משמעותי. עולם אבטחת המידע והסייבר ממשיך לצבור תאוצה וכפועל יוצא כך גם חשיבות ונחיצות מערך ה-SOC עולה והופכת למשמעותית הרבה יותר. אם מסתכלים במבט לשנתיים אחורה אזי שכמות האיומים עולה בהדרגתיות ובהתאם לכך גם כמויות המוצרים בשוק הסייבר.

אוראל: ככל שהשנים עוברות ככה אנחנו נחשפים לפגיעויות מסוכנות ומתוחכמות יותר ויותר, למעשה- ע"פ הסקרים בעולם קצב הגדילה של תקיפות סייבר עם השנים גדל באופן אקספוננציאלי. קיימות פגיעויות שלא עולות על כל דמיון. לדוגמא- שליטה מרוחקת על רכב, חיסול בן אדם ע"י פריצה לקוצב הלב שלו ועולם שלם של רכיבי IOT פגיעים, כל זה מוביל למסקנה המרכזית- אי אפשר להישאר מאחור ולהשאיר את הארגון חשוף וללא יכולת הכלה למתקפות בזמן אמת.

האם כדאי להוציא את ניהול ה-SOC למיקור חוץ?

אבירן: לדעתי לא. בין השאר מהחשש לחשיפת המידע הרגיש בפני גורמים חיצוניים והיתרון בשימור הידע הקיים בתוך הארגון.

אוראל: אין תשובה נכונה לשאלה הזו, כל ארגון ומה שמתאים לו מבחינה תקציבית ופתיחות ארגונית באופן עקרוני אין נוסחת קסם להגנה על ארגון כל פתרון חייב אינדיבידואלי לצרכי הארגון.

מהי התחזית שלך למפת איומי הסייבר לשנת 2018?

אבירן: איומי הסייבר משתנים בין אופי הארגון לבין גורם האיום היחסי, האיומים משתנים בתדירות ואפשר להבחין במגמת עלייה בכל הקשור להונאות ו/או תקיפות מבוססות הנדסה חברתית, זה לצד היכולות הטכנולוגיות המתפתחות מאפשרות איומים שונים ומגוונים.

התחזית היא למגמת עלייה. בעיקר בעולמות ה Phishing ו- IOT. רואים זאת בהתחמשות הארגונים הגדולים בכל נושא הגנת הסייבר, בישראל בפרט ובעולם בכלל.

אוראל: ללא ספק העולם צועד לכיוון ה IOTו Smart city מה שמגדיל את טווח האפשרויות של התוקף. בנוסף- עולם ה- SCADAעצם החשיבה על אפשרות השליטה בתשתיות אנרגיה, מים וגז של מדינה מהווה תשתית תקיפה מאוד מפתה למדינות וקבוצות האקרים גדולות.

מהי הדרך הטובה ביותר להימנע ממתקפות סייבר?

אבירן: הדבר הראשון הוא מודעות העובדים בארגון באשר לסכנות הקיימות ואיך להימנע מהן. כוח אדם איכותי ומקצועי, בניית נהלי תגובה לשלל אירועים, ובחינת ניהול סיכונים מתמדת בהתאם למורכבות והאתגרים החדשים ברשת.

ההון האנושי בשילוב יכולות טכנולוגיות מתקדמות הינן מנגנון מנצח אל מול מפת האיומים המשתנה.

אוראל: אין דרך להימנע ממתקפות סייבר. השאיפה של כל ארגון היא לגלות את המתקפה כמה שיותר מוקדם ולהכיל אותה במינימום זמן לפני שהיא עושה נזק בלתי הפיך לארגון.

ביצוע תרגול מתמיד של צוות ה-SOC, הגדלת מודעות עובדים בארגון, הפצת מייל Phishing יזום והעלאת מודעות להנדסה חברתית ולבסוף ביצוע Risk Managementוהבנת צרכי הארגון.

במידה וארגון מותקף, כיצד ניתן להתאושש ביעילות ממתקפת סייבר?

אבירן: זיהוי מהיר של וקטור התקיפה ובלימתה מוקדם ככל האפשר ע"י פעולות מנע. וידוא סיום המתקפה ובחינת היקף הנזק שנגרם לארגון. התאוששות, למידת מתאר התקיפה ו ה ס ק ת



מסקנות לצורך מניעה עתידית.

אוראל: כל ארגון חייב סט פעולות לתרחיש "יום הדין" דרכי שרידות והתאוששות תכנוןBCP מפורט ומדויק. הארגון חייב להכין את עצמו מבעוד מועד לתרחיש מהסוג הזה עם גיבויים למקומות קריטיים תוכנית התאוששות ואסטרטגיית מניעה עתידית של תקיפות דומות כל יום שעובר ללא תוכנית התאוששות מתקיפה הוא הימור על חיי הארגון להיות בעל זמן תגובה מהיר ויעיל למתקפות בזמן אמת הכלתן והפקת חסימות רלוונטיות

מהן המגמות החמות בתחום הסייבר?

אבירן: כמו תמיד עולם ה-Phishing, בייחוד בניסיונות "ליירט" בכירים בארגון באפיק הדואר האלקטרוני. איומי כופרה תמיד מרחפים מול ראשם של ארגונים (על אף שחלה ירידה קלה בהשוואה לשנה החולפת).

IOT, מתקפות מניעת שירות בנפחים משמעותיים, דלף מידע עסקי וניסיונות הונאה.

אוראל: הפיכה מ-ניצוד לצייד, ביצוע פעולות פרואקטיביות בארגון, בניית Automations לסוגי ההתקפות המגוונות ביצוע פרויקטים ומשימות בעולם ה- Hunting פיזור Honeypots ו Deceptions ביצוע קורלציות עם מערכות Big Data וחיפוש סטטיסטי המבצעות קורלציות בין אירועים שונים לכדי יצירת מתאר מתקפה. מוצרי אנומליה המזהות דפוס התנהגות חשוד (ע"ח מערכות מבוססות חתימות). חיבור ממשקי המודיעין .

אוראל: מערכת שהיא Big data & Machine learning אשר יודעת להכיל אירוע ולבצע את כל הפעולות האוטומטיות הנדרשות להקל ולחסוך זמן למערך ה-SOC ולחוקרים לבצע חקירה מעמיקה וחיזוק הגנה להפוך את מרבית העיסוק של המערך לצייד. הרמת תשתיות למלכודות חדשות וביצוע Hunting.

מהם האתגרים העיקריים הניצבים בפני מנהל ה-SOC בעידן הסייבר של היום?

אבירן: האתגר הגדול הוא ביכולת לנהל אנליסטים מקצועיים והבאתם למצב של מוכנות שיא לכל אירוע סייבר פוטנציאלי. בנוסף חשוב ללוות את תהליך בניית ההתראות והבאת המידע המקסימלי שניתן להפיק מכל אירוע. חשוב לראות בפרספקטיבה רחבה את הסטטוס הקיים, מה נדרש לשפר לצורך השגת אפקטיביות מרבית. מוכנות, מקצועיות, התמודדות . למידה מתמדת.

אוראל: כיום, מנהל SOC צריך לשלוט בהמון עולמות תוכן, להיות מוכן לכל תרחיש תקיפה אפשרי לדעת להכיל אותו ולפעול בהתאם. ווקטורי התקיפה בכל רגע רק גדלים ומתרחבים ומנהל ה-SOC חייב לדעת במה למקד את הצוות ועד כמה להיכנס עמוק לפרטים להיות בעל יכולת תגובה מהירה, יכולת ניהול אירוע, עמידה במצבי לחץ ותמיד להיות Up to date לתקיפות חדשות.

מה לדעתך הידע הנדרש היום מהבקרים ב-SOC? ומצוותי התגובה?

אבירן: בקרי ה-SOC נוגעים במגוון נושאים ולכן נדרש ידע מגוון המתחיל באבטחת מידע והכרות עם עולם מתקפות הסייבר, ידע בתקשורת, ניהול רשתות ואף הכרה בסיסית של קוד תוכנה. בנוסף חשוב שיהיו לו כישורים חברתיים, סמכותיות, הגדלת ראש ועמידה במצבי לחץ.

אוראל: הבקרים חייבים להיות עם ידע בסיסי בSecurity הכרת ממשקי אבטחה וידע בפיתוח. צוותי התגובה חייבים להיות מורכבים מאנשים עם ידע נרחב, כשב-TOP שלו נמצאים חוקרים מנוסים עם ידע נרחב ב- Digital forensics, Malware analysis, Programing languages,Windows & Linux internals.

האם ניתן לומר שחלה עלייה במודעות הנהלות הארגונים בנושא אבטחת המידע והגנת הסייבר?

אבירן: בהחלט. הסביבה מודעת הרבה יותר לנושא רגישות אבטחת המידע וזה בא לידי ביטוי בהתנהלות העובדים בארגון, ביידוע והבנה במקרים הנראים עבורם חשודים והם דואגים להציף את זה בפני הגורמים הממונים.

אוראל: כמובן שקיימת עלייה רבה במודעות בניית נהלים רבים וטובים אך יש עדין יש ארגונים בעלי פערים רבים. לא כל ארגון מבין את החשיבות של אבטחת מידע בארגון שלו ולכן חלוקת התקציב קטנה יותר ומוטעית. לאחר שעושים את ה-BCP הנכון מבינים שהשקעה באבטחת מידע בארגון היא מהלך נחוץ וחיובי.

תקיפה על שרשרת האספקה

למה זה צריך להדאיג אותנו?

שיחה עם חברי האיגוד העולמי לאבטחת מידע (ISSA)

בעידן הסייבר של היום, החוליה החלשה בשרשרת האבטחה יכולה להימצא דווקא בהתקשרות ובחיבורים של הפעילות העסקית של הארגון עם שותפים עסקיים וספקים. שוחחנו עם מספר מומחים מהאיגוד העולמי לאבטחת מידע (ISSA), ולהלן התובנות שלהם בנושא.

מתקפת שרשרת האספקה מתרחשת כאשר גורם עוין מצליח לחדור למערכות המחשוב של הארגון באמצעות ספק או שותף עסקי חיצוני שמחובר למערכות המחשוב של הארגון, או אשר מחזיק במידע רגיש עבורו. ותופעה זו השתנתה פלאות בשנים האחרונות, כאשר יותר ויותר גורמים צד ג' (ספקים, שותפים עסקיים, וכו') מחזיקים במידע רב או שניגשים אל תוך מערכות הליבה של הארגון מרחוק.

הסיכון שנובע מכך הינו גבוהה וממשיך בעוד שתופעה זו ממשיכה לצבור תאוצה בקרב התוקפים, שמנצלים את הקישוריות "האחורית" לרשת של הארגון המותקף. היתרון בדבר, הוא בכך שלאור הפופולאריות של המתקפות באמצעות שרשרת האספקה, הרגולטורים התחילו לגלות עניין בתופעה זו, והחלו לבנות מסגרות וסטנדרטים כיצד למזער את הסיכון שנובע משרשרת האספקה.

ובנתיים, התוקפים ממשיכים לחגוג, ומפתחים ארסנל כלים לביצוע תקיפות מתוחכמות ומטורגטות יותר לכיוון ארגונים ספציפיים.

ולאלו שהתופעה אינה ברורה עדיין, הנה מספר תקריות אבטחה שקרו בעיקר בגלל כשל בשרשרת האבטחה של הספקים צד ג', אשר גרמו לחורים בשרשרת האבטחה של הארגונים עצמם שהיו מטורגטים למתקפות הסייבר.

תקרית מתקפת הסייבר ע TARGET

המקרה המפורסם של מתקפת הסייבר שאירעה על ענקית הקמעונאית TARGET, החלה בגלל חולשות והיעדר אבטחת מידע נאותה בספק שסיפק שירותי מיזוג אוויר (HVAC).

תקרית מתקפת הסייבר על EQUIFAX

חברת EQUIFAX האשימה ספק תוכנה צד שלישי, שסיפק להם מערכות מחשוב, ואשר היו להם ולשות רבות במערכת שבה EQUIFAX השתמשו. ואז המשכיו בהאשמות לספק נוסף אשר הורידו קובץ זדוני מרשת האינטרנט והצליח להדביק את המחשבים בארגון בנוזקה.

תקרית זליגת מידע של חברת PARADISE PAPERS

תקרית מצערת שבה מעל 13 מיליון רשומות שמכילות מידע רגיש אודות נתוני מס וכספים של ארגונים גדולים, פוליטיקאים וסלבריטי בארה"ב דלפו לרשת האינטרנט. והמקור של הדליפה? נכון – המקור של הדליפה היה זה משרד עו"ד שטיפל בניירת, והוא זה שהיה החוליה החלשה בשרשרת האבטחה.

תקרית זליגת מידע של חברת PANAMA PAPERS

עוד תקרית מצערת שבה מיליוני רשומות שמכילות מידע רגיש דלפו לרשת האינטרנט. והמקור של הדליפה? נכון, המקור של הדליפה היה זה משרד עו"ד שטיפל בניירת, והוא זה שהיה החוליה החלשה בשרשרת האבטחה. מה שמראה שההיסטוריה חוזרת על עצמה, וארגונים נכשלים בתהליך הפקת הלקחים.

ומה שעצוב הוא שלא מדובר במקרים בודדים, אלא בתופעה של ממש. עפ"י מחקר שבוצע ע"י חברת Ponemon, כ-56% מהארגונים שנפלו קורבנות למתקפות סייבר, הסיבה העיקרית הייתה ספק צד שלישי. נתון נוסף שעולה מהמחקר, הוא שכמות הארגונים צד ג' שמחזיקים מידע רגיש או שיש להם גישה למערכות המחשוב ו\או מידע רגיש עלה בכ-20%.

עוד נתון מדאיג, הוא שרק 35% מהחברות החזיקו ברשימה של כל החברות צד ג' שאיתן הם עובדים ומשתפים מידע, בעוד שרק כ-18% מהחברות ידעו שהספקים צד ג' שלהם מעבירים נתונים הלאה לספק נוסף (צד ג' של צד ג'). וזה מהווה בעיה רצינית, היות וללקוחות לא ממש משנה האם המידע שדלף היה מהארגון או מהספקיות צד ג' של הארגון. עבירה על החוק היא עבירה על החוק.

והבעיה לא נגמרת ברגע שהארגונים מסיימים את ההתקשרות עם אותם ספקים. בסתיו האחרון, רשת הענקית של דומינוס פיצה באוסטרליה ספגה מכה כתוצאה מאירוע סייבר של ספק ישן שלה, שככל הנראה החזיק במידע רגיש של פיצה דומינוס, וזה דלף החוצה במסגרת מתקפת סייבר על הספק עצמו, מידע שהכיל שמות של לקוחות, פרטי התקשרות, כתובות ודוא"ל.

"ארגונים רבים אינם מיישים מסגרת נאותה של ניהול סיכונים לשרשרת האספקה של הארגון, מה שמקשה על תהליך אבטחת הנתונים בתהליך הפסקת חוזה התקשרות עם ספקים", אמר יניב מילחוביץ, סמנכ"ל חברת הייעוץ טיטנס סקיוריטי בע"מ.

"יתרה מכך, הרבה ארגונים אינם בודקים את רמת אבטחת המידע גם בעת תהליך העבודה עם ספקים צד ג', כאשר חוזה ההתקשרות עדיין בתוקף. מי יודע מה קורה ברשת של הספק? היכן יושב המידע? למי יש גישה למידע? הרי אנחנו יודעים שמידע רגיש יכול לדלוף החוצה, ונדע על זה זמן רב לאחר מכן, ואף יתכן מצב שבו הארגון כבר לא בקשרי התקשרות עם אותו ספק", הוסיף שלומי מרדכי, סמנכ"ל התקשו"ב של הקריה האקדמית אונו, ומשנה לנשיא האיגוד העולמי לאבטחת מידע (ISSA) – הציאפטר הישראלי.

כעת, הרגולטורים החלו להסתכל בעיון רב יותר ולבחון את הסיכונים הנובעים משרשרת האספקה של הארגון. בשנה האחרונה, הרגולטור המגזר הפיננסי של מדינת ניו יורק החל לחייב ארגונים פיננסיים שפעילות בניו יורק לוודא שהם מנהלים את סיכוני הסייבר של שרשרת האספקה שלהם.

בעוד כחודש, האיחוד האירופאי יעשה דבר דומה, באמצעות החקיקה החדשה של ה-GDPR, שמחייבת את כל הארגונים שאוספים נתונים רגישים אודות אזרחי אירופאיים, לדאוג לרמת אבטחה נאותה, כולל היבטים של הגנה לאורך כל שרשרת האספקה של הארגון.

"עבודתם של הרגולטורים בתחום ניהול הסיכונים בשרשרת האספקה עוד בחיתוליו, ומרבית הארגונים אינם מכוסים מבחינת ניהול הסיכונים שנובע משרשרת האספקה", אמר דני אברמוביץ, מנכ"ל חברת הייעוץ טיטנס סקיוריטי, ונשיא של האיגוד העולמי לאבטחת מידע (ISSA) – הציאפטר הישראלי. " ארגונים מהמגזר הפיננסי החלו בעשייה ומצב יחסית טוב לשאר השוק", הוא הוסיף. "אבל ארגונים רבים אחרים אינם מבינים כלל את הסיכון, ואינם ערוכים להתמודד בצורה נאותה אל מול האיומים שנובעים משרשרת האספקה, ואנחנו הולכים להיות עדים לתקריות סייבר נוספות בעתיד הקרוב", אמר דני.

עפ"י תחזיות של חברות מחקר, עולה כי הרגולטורים יתחילו לדרוש מהארגונים לנהל בצורה נאותה יותר את סיכוני הסייבר שנובעים משרשרת האספקה. "מדובר בטרנד שהולך וגובר", אמר יניב.

הסיכונים טמונים בשימוש בחומרה ותוכנה של חברות צד ג'

כיום, כל החברות עושות שימוש בתוכנה וחומרה של חברות צד ג'. אף ארגון לא מפתח טכנולוגיות מאפס, וזה תודות לתוכנות שמבוססות על קוד פתוח, וגם על המגוון העשיר של שירותי הענן. אבל תופעה זו טמונה בה גם סיכון רב. כל שירות או תתוכנה שמורידים או עושים בה שימוש, צריכה להיבדק, ולהיות מנוטרת לזיהוי נקודות חולשה, ופגיעויות אלו צריכות להיסגר מבעוד מועד.

באפריל שנה שעברה, חוקרים אבחה של חברות Flashpoint Intelligence, דיווחו על תופעה שבה פושעי סייבר החלו במתקפות ממוקדות על פלטפורמת ecommerce של Magento, שמבוססת על קוד פתוח. התקיפות כללו בין היתר ניסיונות גניבת מספרי כרטיסי אשראי, והתקנת נוזקות לטובת כריית קריפטו. החוקרים גילו שלפחות 1,000 טבלאות ניהול מערכות דלפו לרשת השחורה, כאשר עפ"י שירותי מודיעין סייבר, האנליסטים גילו שישנו

ביקוש רב ברשת השחורה לנתוני גישה לפלטפורמה הזאת ספציפית.

בנוסף, התגלה עניין רב בפלטפורמות נוספות כגון Poerfront CMS וגם ב-OpenCart.

בשנה שעברה, פגיעות CSRF בגרסת ה-Magento Community הותירה אחריה 200,000 רשתות קמעונאיות פגיעות למתקפה זו. תוקפים אשר הצליחו לנצל פרצה זו, קיבלו גישה מלאה למערכת, מה שחשף את הבסיסי הנתונים בפני התוקף, מידע שהכיל נתונים רגישים של לקוחות החברות השונות.

מאחר שהגרסה המסחרית של התוכנה משתמשת באותו קוד, קיים היה חשש שגם ארגונים אחרים אשר עושים שימוש בפלטפורמה המסחרית, יפלו קורבנות למתקפה זו.

הבעיה היא יותר חמורה ממה שארגונים חושבים. לא רק שהמידע של הארגון ולקוחותיו נמצא בסיכון גבוה, אלא, אם הפגיעות מוטבעת בתוך מרכיבי תוכנה או חומרה, זה יכול להוביל לבעיות נוספות בעתיד. למשל, רכיב CPU של מחשב שמזוהם בנוזקה שמאפשרת גישה אחורית למערכת, מערכות צילום (CCTV) ללא הזדהות ואימות חזקים, או מרכיבי תוכנה שאינם מאובטחים – כל אלו יכולים לגרום נזק רב בעתיד.

למשל, כולנו זוכרים את הבאג הנודע של Heartbleed, שהשפיע על מיליוני אתרים והתקנים ניידים, כמו גם על תוכנות של הספקיות הגדולות ביותר במשק וביניהם Oracle, VMWare ו-Cisco.

"מה שמדאיג אותנו זה ניסיונות שינויים לא מורשים במידע, ריגול תעשייתי (הן ברמת מדינה והן ברמת ארגונים מסחריים), וכמובן גם פגיעה בזמינות המערכות, בייחוד של מערכות קריטיות", אמר שלומי. למשל, קרו מקרים בהם מרכיבי חומרה ותוכנה שנדבקו בקוד זדוני או הוחלפו בחלקים זדוניים, בכוונת תחילה, כך שתוקפים הצליחו לעקוף את מנגנוני ההגנה באמצעות שימוש ותקיפת שרשרת האספקה של הארגון, בשל היותה פחות מאובטחת מהרשת של הארגון הנתקף.

מרבית החברות חוששות מלאבד מידע רגיש (כגון מידע של לקוחות או קניין רוחני של עצמם) כתוצאה מפריצה שמקורה בגורם צד ג', כחלק משרשרת האספקה. ולכן, על הארגונים לנקוט בצעדים על מנת לוודא סגירת פרצות גם בכל תהליך שרשרת האספקה.

ארגון ה-ISO העולמי, פרסם תקן שמספק הנחיות בנושא היבטי אבטחת מידע עם הייחסות ספציפית לשרשרת האספקה. התקן נקרא ISO 28000, והוא שוחרר כבר בשנת 2007, ועבר רענון בשנת 2014 ואושר לפרסום באופן פורמאלי. ארגונים חייבים לאמץ את התקן, או המלצות אחרות (Best Practices) על מנת לחזק את שרשרת אבטחת המידע של הארגון בצורה נאותה, ולא להשאיר שום חוליה חלשה או פרצות שעלולות להוביל לזליגת מידע כתוצאה מאירועי סייבר.

מעונן חלקית
סיכוני סייבר במחשוב ענן



העולם כפי שהכרנו כבר לא קיים, וכיום, מרבית הארגונים בעולם מתבססים על תשתיות מחשוב של ספקיות הענן, עם מעט מאוד כח עיבוד ומערכות מחשוב מקומיות (On-Premise). זה מוביל אותנו לאמץ אסטרגטיה וגישת אבטחה שונה, שבה הארגון מנסה להגן על המידע הרגיש שלו, אבל מידע זה לא נמצא בין כותלי הארגון, אלא באתרים מרוחקים – אצל ספקיות הענן. "והתוקפים מתוחכמים", אומר שלומי. הם תוקפים את החוליות החלשות ביותר בשרשרת".

"אפילו החומרה כעת מבוססת מחשוב ענן" אמר יניב. "ההגדרות ברירת המחדל של כלי ריתוך במפעל לייצור מכוניות, שמבוסס על טכנולוגיית IOT, מאפשר שליחת נתונים דיאגנוסטיקה לחברות הייצור של המכוניות, במטרה לאגור ולנתח נתונים אלו, ולחזות בעיות תחזוקה בעתיד", יניב הוסיף. "בעוד זה נשמע ממש מגניב, זה גם מהווה פירצה חמורה, ומעין דלת אחורית למערכות המחשוב של סביבת העבודה במפעל הייצור".

חברות שמספקות שירותים שונים אינן מאובטחות מספיק

"כולנו מכירים את האימרה" חוזק השרשרת נמדד עפ"י החוליה החלשה שלה", אומר שלומי. תהליך העבודה עם שרשרת האספקה נהיה חלק אינטגראלי בכל פעילות עסקית של כל ארגון בעידן של היום, עידן שבו הקישוריות הדיגיטלית והחדשנות הולכת וגוברת מדי יום.

אבל עלינו להבין את מהות הסיכון, ולגבש מתודולוגיה ותפיסה כיצד לנהל את הסיכון הזה בצורה הטובה ביותר, כך שנוכל למזער את הפגיעה בפעילות העסקית של הארגון, שנובעת מההקשר של שרשרת האספקה.

לפני כחצי שנה, חברת שיווק בשם Deep Root Analytics, ששימשה את המועצה הלאומית של הרפובליקנית בארה"ב, נפלה קורבן למתקפת סייבר שבו דלפו נתונים רגישים של למעלה מ-200 מיליון מצביעים. אנשי ה-IT של החברה, אחסנו (ככל הנראה בטעות) את הנתונים הרגישים על שרת שהיה פתוח לציבור (רשת האינטרנט), מה שהקל מאוד על התוקפים מלגנוב את המידע.

אבל גם חברות גדולות יותר פגיעות למתקפות סייבר מסוג זה. כולנו זוכרים את המקרה של חברת Verizon, אשר נפלה גם היא קורבן למתקפת סייבר, שבה דלפו כ-6 מיליון רשומות של לקוחותיה. הדליפה נגרמה כתוצאה מפגיעות במערכות של NICE, ספקית שירותי תוכנה של החברה.

אבל לא לשכוח, שכשמדובר באירועי סייבר, אף אחד לא נשאר ללא פגע. גם חברת DELOITTE הענקית נפלה קורבן למתקפת סייבר בסטמבר האחרון, מתקפה שבה התוקפים הצליחו לקבל גישה למיילים ותוכניות חסויות אחרות של הלקוחות VIP של דלוייט. עפ"י דיווחים שונים, התוקפים הצליחו לקבל גישה למערכות כתוצאה מבקרת גישה והרשאות לקויות מצד אנשי ה-IT של החברה.

בעוד שזה לא ברור האם חברת דלוייט הייתה המטרה העיקרית, או שהתוקפים ניסו להגיע למטרות אחרות שהיו לקוחות VIP של דלוייט, אנחנו צפויים לראות עוד מתקפות סייבר נוספות בעתיד הקרוב, כתוצאה מניהול סיכונים לקוי של שרשרת האספקה של הארגון.

כיצד לנהל נכון את הסיכונים של שרשרת האספקה?

מחקרים מראים, שניהול סיכונים נכון של שרשרת האספקה, מניב תוצרים לא רק מבחינת עמידה בדרישות הלימה לתקינה ורגולציות שונות, אלא גם מצליח למזער את הסיכון של מימוש תקיפה, או לפחות למזער את מידת ההשפעה באם התקיפה הצליחה להתממש. חברות המחקר מראות כי ניתן למזער בכ-20% את הסיכון לתקיפות סייבר כתוצאה מניהול נכון של היבטי אבטחת המידע בשרשרת האספקה של הארגון.

אז מה נדרש מאיתנו לעשות? האמת היא שזה די פשוט. ריכזנו לפיכם מספר המלצות מפיהם של מומחי אבטחת מידע ומנהלי אבטחת מידע מהמובילים במשק:

טיפ 1: מיפוי וסיווג כלל הספקים

המשימה הראשונה שצריכה להיות הינה למפות את כלל הספקים שמספקים שירותים שונים לארגון, ולסווג אותם לפי 3 או 4 רמות:

- ספק מחזיק – מדובר בספק שמחזיק מידע של הארגון.
- ספק ניגש – מדובר בספק שניגש למידע או מערכות מידע של הארגון.
- ספק משולב – מדובר בספק שגם מחזיק וגם ניגש למידע או מערכות מידע של הארגון.
- ספק כללי – מדובר בספק כללי, שלא אמור לגש למידע או מערכות מידע, כגון ספק שירותי מיזוג אוויר, תשתיות חשמל, טלפוניה, ניקיון, ושירותים כלליים אחרים.

את המיפוי ניתן לעשות עם אנשי הרכש בחברה, אנשי ה-IT, וגופים נוספים אשר צורכים שירותים חיצוניים כגון תפעול, ייעוץ משפטי ועוד.

טיפ 2: מסגרת לניהול סיכונים לשרשרת האספקה

חשוב לגבש מסגרת לניהול והערכת סיכונים לשרשרת האספקה. צריך להגדיר רמות סיווג לסיכון לפי סוג הספק והשירות שניתן. לאחר מכן, לכל ספק, צריך להגדיר רמת סיכון, בהתאם לסוג השירותים אותם הוא מספק (זה ייחודי לכל ארגון וארגון), ולהתחיל לנהל את הסיכונים בהתאם.

חשוב לנהל יומן סיכונים (Risk Register) של כלל הספקים, ולתעדף את הטיפול לאותם ספקים אשר נמצאים ברמת סיכון גבוהה.

טיפ 3: מסגרת לניהול אבטחת המידע

לאחר שגיבשנו מסגרת לניהול סיכונים בשרשרת האספקה, חשוב לאמץ מסגרת לניהול אבטחת המידע של שרשרת האספקה. מסגרת זו תספק לארגון הנחיות והמלצות כיצד לחזק את רמת אבטחת המידע של שרשרת האספקה, ובכך לעבות את רמת הבשלות של אבטחת המידע של כלל הארגון. ניתן להיעזר בתקן ISO 27001 (בייחוד לאלו שכבר החלו בהטמעת התקן או שכבר הוסמכו לתקן), וגם מומלץ להוסיף את המעטפת ההגנה כפי שממליצים בתקן ISO 28000, תקן שדן באופן ייחודי בניהול אבטחת המידע בשרשרת האספקה של הארגון.

טיפ 4: תאימות והלימה למדיניות ונהלי אבטחת המידע של החברה

לא די לבחון את מסמכי המדיניות ונהלי אבטחת המידע שקיימים אצל ספקיות צד ג' (בהנחה שאלו בכלל קיימים), אלא חשוב להכניס את זה להסכמי השירות והחוזים, שעל הספקים להתחייב לעמוד (במידת האפשר) בדרישות אבטחת המידע של הארגון, כלומר, על ספקי השירותי ליישר קו עם מדיניות ונהלי אבטחת המידע של הארגון עצמו. זה שימושי עוד יותר כאשר מדובר בספקים קטנים, שאין להם כלל מסמכי מדיניות ונהלים, אז הם ישמחו לקבל מהארגון את התיעוד המתאים לכך.

טיפ 5: סקר אתר תקופתי

חשוב להכניס את הנושא הזה כבר בהסכמי ההתקשרות והחוזים מול הספקים. ניהול סיכונים בתהליך אבטחתה מידע אינו זבנג-וגמרנו, אלא מדובר בתהליך הוליסטי, דינאמי, ומתמשך. חשוב לדרוש את היכולת לאפשר לכם לבצע סקר אתר אחת לתקופה (בהתאם למידת הרגישות של המידע וסוג הספק – ספק מחזיק, ספק ניגש, ספק כללי או משולב). מטרת הסקר הינה "להלחיץ" את הספק ולגרום להם להבין שמישהו בודק אותם מדי פעם, ורצוי גם בהפתעה, וגם באמת לבדוק אחת לתקופה מה הסטטוס של אבטחת המידע באתר הספק.

במקרים מסוימים, ניתן גם להסתפק בהתעדה של הספק לתקנים כגון ISO 27001, SOC2 או מענה לשאלוני אבטחת מידע שנשלחים מעת לעת. במידת הצורך, חשוב שתהיה אפשרות לארגון לבצע סקר באתר הספק. ישנם ספקים שדי לעשות סקר אתר פשוט (מבוסס על תשאול ואבחון תצפיתי של מערך אבטחת המידע בארגון), וישנם ספקים שלא די בכך, ויצטרכו לבצע מבדקי חוסן, סקרי סיכונים מעמיקים, ואף בדיקות קוד לתוכנה. הכל תלוי כמובן בסוג הספק, ורמות הסיכון שנובעים מהפעילות שלו כלפי הארגון.

חשוב לנהל מעקב (Risk Register) נאות אודות מתי בוצע הסקר, ע"י מי, מה זה כלל, מה היו הממצאים, מי מטפל בממצאים, מהו תאריך היעד לסגירת הממצאים, כיצד מוודאים סגירת הממצאים, וכדומה.

בנוסף, ישנן חברות נוספות שמספקות שירותי הערכת סיכונים לשרשרת האספקה כגון BitSight Technologies, SecurityScorecard, ואף ספקיות כחול לבן כגון Rescana ו-Panorays. החברות הללו מספקות שירותים שבוחנים את הספקים מבחוץ, ומדרגים אותם עפ"י רמות מידע של ציונים של עמידה בדרישות אבטחת מידע בהתאם למדרג של אותו מגזר (למשל פיננסי, ממשלתי, היי-טק וכו').

בנובמבר האחרון, מספר חברות מובילות במגזר הפיננסי, כגון American Express, Bank of America, JPMorgan, וגם Wells Fargo חברו יחד והכינו שירות ייחודי של הערכת ספקים שנקרא בשם TruSight.

חברות אחרות כגון Barclays, Goldman Sachs, HSBC ו-Morgan Stanley הכריזו שהם משתמשים בשירותיהם של חברת HIS MARKIT לביצוע הערכת סיכונים לספקים.

ישנן לא מעט חברות ומערכות שיכולות לסייע לכם בניהול סיכוני הסייבר שנובעים משרשרת האספקה, ואנחנו ממליצים בחום להתחיל לגבש לכם מתודולוגיה ומסגרת עבודה לניהול הסיכונים עוד היום, על מנת שתוכלו למזער את הסיכונים שעלולים לקרות מהאירועי סייבר שעתידים להגיע.



מה למדתי מעבודתי ב-SOC?

שיעור 1

אין דבר כזה SOC מושלם

כאשר אתם חושבים על מרכזי SOC (ר"ת של Security Operation Center), מה אתם מדיינים לעצמכם? חדר שבו ישנן מערכות ניטור שעובדות 7/24? חדר מלחמה מפואר עם עשרות מסכים בהם מוצגים מפות איומים ענקיות?

כאשר התחלתי את הקריירה שלי ב-SOC, עבדתי כאנליסט בחברה שסיפקה שירותי SOC מונהלים (MSSP). עבדתי בתוך צוות שסיפק שירותי ניטור של אירועי אבטחת מידע וגם סיפקנו בין היתר שירותים הנדסיים ללקוחות החברה. היה לנו את החדר מלחמה המפואר, כח אדם ייעודי, ומגוון מערכות ניטור.

מנקודת מבט אחת, בגלל שחייבו אותנו לספק את השירותי ניטור הטובים ביותר עבור הלקוחות שלנו, היה לנו מזל גדול. היו לנו המון מערכות וכלים שבהם התנסינו. היה לנו תקציב כמעט לא מוגבל, והמון צוותים מוכשרים שעבדו אצלנו ב-SOC. עם זאת, כשעבדנו כשותף חיצוני עבור הלקוחות שלנו, היו כמה מגבלות עבור הארגונים להם סיפקנו שירותי SOC מנוהלים, כמו גם עבור הצוותים שלנו.

לדוגמה, מאחר שסיפקנו בעיקר שירותי ניטור ומעקב עבור ארגונים חיצוניים, הפעילות שלנו הייתה מוגבלת במרבית המקרים מבחינת היכולת שלנו להגיב, כמובן מעבר להתראות והמלצות למימוד. מאידך גיסא, צוותי הבקרים והתגובה במרכזי SOC פנימיים יכולים לספק שירותים מעמיקים נוספים כגון שירותי תחקור דיגיטלי, שירותי ניתוח נזקות ומתקפות מתוחכמות, וכל זה באמצעות מגוון כלים ושיטות עבודה בשילוב עם תהליכים סדורים של תגובה לאירועי סייבר (בהתאם לתרחישים שונים), ולכן גם היכולת שלנו להשפיע על ביצוע התהליכים הללו בתוך הארגון היה גדול יותר מאשר רק לספק שירותי התראות וניטור חיצוניים.

הנקודה שלי, זה שאין SOC מושלם. כל צוותי העבודה (בקרים, אנליסטים, תגובה, תחקור דיגיטלי וכו') פועלים תחת מגבלות של תקציב, משאבים, ופוליטיקה ארגונית או אילוצים אחרים שקיימים בכל ארגון מודרני. ולא לכל ארגון יש את הטכנולוגיה ואת הידע או הכח אדם הנדרש כדי להרים פעילות SOC ולנטר את מערך המחשוב שלו למקרה של זיהוי ותגובה לאירועי סייבר. ארגון ה-SANS העולמי, מגדיר את הצוות SOC האולטימטיבי, שמורכב ממגוון בעלי תפקידים כגון: בקרים, אנליסטים, מהנדסי מערכת, ציידי איומים, חוקרים, מומחי פורנזיקס, וצוותי תגובה. לעתים קרובות, ישנו גבול דק וערפול מסוים מבין בעלי התפקידים הללו, וזה תלוי בסוג הארגון, בגודלו, תרבות ומבנה ארגוני, ופרמטרים נוספים כגון אילוצים תקציביים. וכמובן, לא לכל הארגונים יש חדר מלחמה מפואר, עם עשרות מסכי פלזמה שמציגים מפות איומים ומערכות ניטור שונות.

שיעור 2

ה-SOC לא יכול לתפקד ביעילות ללא גיבוי מהנהלת הארגון

המטרה העיקרית של ה-SOC היא לזהות ולאפשר תגובה מהירה (כמה שיותר קרוב לזמן אמת) לאיומים ואירועי אבטחת מידע וסייבר. אבל על מנת להגן על הפעילות העסקית, אתה חייב לקבל גיבוי מהנהלת הארגון (מהצד העסקי).

צוותי אבטחת מידע, להבדל מצוותים אחרים כגון פיתוח או מכירות, אינו מייצר הכנסה או נכסים אחרים בעלי ערך רב בעיני הארגון, אלא תומכים בפעילות העסקית של הארגון באמצעות שיטות, בקרות ותהליכי עבודה שנועדו לאפשר רציפות תפעולית, למרות מתאר איומי הייחוס שחלים על הארגון. צוותי אבטחת המידע מתחזקים, מתפעלים ומנהלים את פעילות אבטחת המידע, שמאפשרת המשך פעילות עסקית תקינה בארגון. ניתן לומר שמנהל אבטחת המידע בארגון הוא Business Enabler. ולכן, על מנת שנוכל לטפל בצורה טובה יותר בפעילות העסקית של הארגון, ולאבטח אותה כך שנוכל למנוע מאיומי הסייבר לפגוע בה, או לפחות למזער את הסיכון לכך, אנחנו חייבים שיתוף פעולה מהגורמים העסקיים בכלל, ומהנהלת הארגון בפרט, על מנת שנוכל לבצע את העבודה שלנו בצורה יעילה ואפקטיבית. חשוב לשווק ולמכור לגורמים העסקיים את חשיבותה וחלקה של אבטחת המידע ברציפות התפעולית של הפעילות העסקית בארגון. ללא תרבות ארגונית נאותה, שבה הנהלת הארגון מבינה את הצורך במימוש מערך הגנה הולם, ושיתוף פעולה פורה בין צוותי אבטחת המידע לצוותי הניהול בארגון, פעילות ה-SOC לא תצליח להתרומם כמו שצריך, והיא תשאר לרגלי ההר...ללא תרומה ממשית לארגון.

כמה פעמים ראיתם דוחות חוזרים ונשנים של פגיעויות במערכות בארגון שמקורם מסורקי פגיעויות (Vulnerability Scanners) כאשר הדוחות הללו לא ממש משתנים מדי חודש, אלא נשארים די על אותה כמות פגיעויות.

בעבודתי ב-MMSP, ראיתי את התופעה הזאת גדלה פי כמה, היות ולא היה מדובר רק בארגון אחד שבחר לא לעשות כלום עם הממצאים של הדוחות הללו, אלא כעת ישנם הרבה מאוד ארגונים שבוחרים להישאר פגיעים, ולהגדיל את משטח התקיפה ע"י כך שלא ננקטים צעדים לסגירת הפרצות (לפחות לא בפרק זמן שנדרש לבצע זאת).

לדוגמה, אם היינו מבחינים בסדרה של מכונות נגועות בנוזקה (כגון וירוס או תולעת), יכולנו רק להסלים את האירוע לאנשים הקשר העסקיים שסופקו לנו (מצד הלקוח). ואז זה היה תלוי בהם התהליך לניהול ותגובה של האירוע. היו ארגונים שהחליטו פשוט להשאיר את המכונות הללו נגועות במשך חודשים פשוט כי לא היה להם מי שיטפל בזה, או שלא התקבלה החלטה מצד הגורמים העסקיים בנודע לאופן הטיפול והתגובה של האירוע. מנקודת המבט שלנו, הצורך בלהטט את אותם אירועי אבטחת המידע שוב ושוב יכול להוביל לכאבי ראש מבחינת היכולת שלנו לנהל את האירועים הללו.

שיעור 3

תהליך בחירת טכנולוגיות חייב לבוא בשילוב גידול במצבת כח האדם ובאפיון וקביעת תהליכי עבודה מתאימים

כמה פעמים ראיתם ארגונים רוכשים מוצרי אבטחת מידע ופשוט משאירים אותם על המדף...תופסים אבק. מניח שדי הרבה....

האם זה הגיוני לרכוש שירותי מודיעין סייבר אם אין לארגון מערכות ניטור, או מערכות הגנה או אף יכולת בסיסית לטפל ולנהל אירועי אבטחת מידע? למה לרכוש מוצרים אבטחת מידע אם אין לארגון כח אדם מיומן כדי לטייב את הפתרונות הללו, או שאין הצדקה עסקית של ממש לרכישת המוצר?

בעבודה שלנו ב-SOC, ראינו לעתים תכופות אמצעי ניטור ובקרה שלא הוגדרו או שלא מטוייבים היטב (עפ"י הצרכים העסקיים של הארגון). רבות מהמערכות הללו יצרו רעש כה רב במערכות הניטור שאספו לוגים, עד שלא היה ניתן לנתח את הנתונים בצורה יעילה, או גרוע מכך, המערכות לא הניבו כלל לוגים ואירועים היות ולא קינפגו או לא הותקנו כמו שצריך. עם זאת, עשרות או מאות אלפי דולרים הושקעו ברכישת המערכות הללו...ללא שום יכולת החזר השקעה (ROI) אמיתית מבחינת הארגון.

תהליך בחירת ורכיתש טכנולוגיות בכל תחום בכלל, ובעיקר בתחום אבטחת המידע והגנת הסייבר צריך להיות מחושב. מוצרים אלו צריכים להקל על הצוות שלכם לעשות את עבודתם, ולא להקשות עליהם עוד יותר. לפני שרצים לרכוש פתרון אבטחה כלשהו, אני ממליץ בחום לבחון את הצורך האמיתי באמצעות הטמעת פתרון דומה, שמבוסס על קוד פתוח, על מנת לבחון את הנחיצות ולהוכיח להנהלת הארגון את הערך המוסף ברכישת המערכת, וכמובן את ההחזר ההשקעה (ROI).

שיעור 4

עייפות החומר כתוצאה ממשימות חוזרות ונישנות

עבודה קבועה בניטור וצפייה במערכות בקרה ולוגים 24x7 יכולה להתיש כמעט כל בן אדם, ולגרום לשחיקה במקום העבודה. עייפות החומר היא גם חלק גדול מהסיבה שעזבתי את עבודתי

מה למדתי מעבודתי ב-SOC? המשך

כבקר ב-SOC, והמשכתי הלאה לתפקיד מעניין יותר של מהנדס מערכות ב-SOC. כאן, התפקיד היה שונה קצת, והתחלתי לאפיין את הצרכים העסקיים עם הגורם העסקי ולאפיין חוקים במערכות SIEM. כעת, באמצעות אפיון נכון של מערכות הניטור (SIEM), עזרתי בעצם לצוותי הבקרים ב-SOC לזהות מהר יעיל יותר התראות וניסיונות תקיפה.

התשת כוחות של הכח האדם שעובד בצוותי הבקרים הינו חלק בלתי נפרד מהמקצוע של בקר, אבל לעתים קרובות אחת הסיבות הנוספות היא גם טעויות אנוש. קל מאוד לאדם שמסתכל על אלפי או עשרות אלפי לוגים ביום לבצע טעות אנוש, ולשגות בתהליך מיון אירועי אבטחת מידע, או אפילו לפספס חלק מהאירועים היות והבקרים מזגזגים בעיניהים מבין מגוון המערכות ב-SOC, עד לנקודה שבה יכולים להפסיק לרגע ולפספס בן רגע את האירועים האמיתיים או הקריטיים.

הנהלת ה-SOC ששואפת לגייס את הצוות המיומן ביותר לעבודה ב-SOC, ואז נותנים להם להביט 24x7 באירועים ולוגים, כושלים בביצוע העבודה שלהם מבחינת שימור עובדים מוכשרים. תהליכים רבים בעבודת הבקרים ניתנים למיכון, ואפשר לתזמן ולהטמיע תהליכי אוטומציה לתהליכי עבודה סטטיים, בהם כמעט ולא נדרשת מעורבות אנושית, ובכך לחסוך מהבקרים עבודה סטטית, ומייגעת של צפייה במיליוני לוגים כל היום.

הנהלת ה-SOC צריכה לשאוף לאתגר את צוותי העבודה (בקרים, אנליסטים וכו') בלספק רעיונות לשיפור היעילות, מהירות ודיוק מערכות הניטור, ולהעצים אותם באמצעות מימוש תהליכים אוטומטיים במערכות ייעודיות.

שיעור 5

התראות ללא טיוב והקשר עסקי מאבדות את ערכן

בעובדתי ב-SOC, כספק שירותים מנוהלים ללקוחות (MSSP), היינו מוגבלים לעתים קרובות מבחינת היכולת שלנו לבצע ניטור של אבטחת המערכות באמצעות כלים שהלקוחות שלנו הטמיעו או פרסו ברשת הארגונית שלהם. כאנליסט ב-SOC, היה זה נפוץ מאוד למשל לראות התראות ממוצרים כמו SNORT, שהפיקו המון התראות שווא כתוצאה מטיוב לא נכון של המערכת, מה שגרם ליצירת התראות שווא או התראות עם מידע חיוני חסר, וחתימות זיהוי מעורפלות שהקשו על היכולת של מערכות ה-SIEM לעשות קורלציה בין המערכות השונות.

כמויות עצומות של התראות שווא נדחפו אוטומטית לתוך "שטח אחסון של התראות שווא", בדיוק כמו דואר ספאם שמועבר אוטומטית לתיקיית זבל, אם כי לעתים קרובות תהיתי כמה מאותן התראות היו למעשה התראות אמיתיות שלא הצלחנו לאמת ולהגיב להם בצורה נאותה.

זו הסיבה שאימוץ גישה ומסגרת ניהול מערך ההגנה שכולל בין היתר יכולות של מערכות ניטור רמת אבטחת המידע ברשת הארגונית, יכולות איסוף וניתוח לוגים, יכולות פורנזיקה מתקדמים, יכולות ניתוח תעבורת הרשת, וזיהוי אנומליה בתחנות העבודה וברשת הינו דבר נחוץ כמעט בכל ארגון שרוצה לגבש לעצמו מערך הגנה הולם על מנת שיוכל להתמודד עם גל איומי הסייבר ההולך וגובר מדי יום.

אם זאת, להגדיר ולממשק את כלל המערכות הללו בתוך ה-SIEM, אינו פיקניק, ואף לפעמים קשה יותר לביצוע מאשר לדבר על זה. וכאן שוב, נכנס תהליך האוטומציה ותזמון של המערכות השונות ברשת הארגון, מה שיאפשר לצוותי התגובה להריץ שאילתות פשוטות עבור ניתוח אירועים שהאנליסטים מבקשים לנתח.

שיעור 6

לפעמים, ידע שבטי אינו ניתן להרחבה

כשעבדתי ב-SOC, אני זוכר שלמדתי המון אודות תהליך תחקור אירוע אבטחת מידע, ע"י כך שישבתי ליד אנליסטים יותר מנוסים ממני ב-SOC, וצפייה בהם בעבודה ביכולת האנליטית וביצוע תהליכי עבודה שונים. אני זוכר גם שלמדתי המון מקריאה בבלוגים ואתרים שונים באינטרנט (כולל פורומים מקצועיים), כחלק מהניסיון שלי לשמור על כשירות מקצועית ולשפר אם הידע והניסיון שלי בתחום.

עם זאת, זאת לא הדרך האידיאלית והיעילה ביותר עבורנו כקהילה לשתף ולחלוק את הידע שנצבר עם השנים, וזה גם לא ניתן להרחבה. כמו כן, מציאת מנחה (מנטור) בתעשיית אבטחת המידע אינה משימה קלה, אלא אם אתה כבר עובד בתעיישה, וישנם מנטורים כאלו במקומות העבודה שלכם שמוכנים לשתף אתכם את הידע שנצבר להם. אם לא, כיצד אפשר לקבל גישה למקורות מידע כדי ללמוד ולהתחיל את הקריירה שלנו בתחום אבטחת המידע?

כקהילה, עלינו ליצור דרכים טובות יותר לתיעוד ולשיתוף תהליכי ונהלי העבודה לתגובה לאירועי אבטחת מידע.

אז מה הלאה?

אני ממליץ לנסות ולהטמיע שיטות עבודה טובות יותר ב-SOC, על מנת לשפר את הידע והיכולות של הכח אדם הקיים, וכמובן לשמר אותו בארגון.

יש הרבה דברים טובים שניתן לחוות ולהשיג באמצעות עבודה ב-SOC, וחלק גדול מהם אני חוויתי ממקור ראשון, אבל באותו זמן יש לא מעט חסרונות כגון העובדה שאתה נדרש לפעול כל הזמן בשיא התפוקה שלך, בעבודה שהיא 24x7 ויכולה להיות די סטטית ומשעממת לפעמים, מה שמגדיל את האחוזים לשחיקה.

על מנת למשוך כח אדם איכותי, ארגונים לא צריכים חדרי מלחמה גדולים ומפוארים, אבל הם כן צריכים ללקט אנשים איכותיים, להטמיע את הפתרונות הטכנולוגיים הנכונים ולבנות תהליכי עבודה שמתאימים לדרישות העסקיות של הארגון (בעיקר אוטומציה של תהליכים).

מתוך הניסיון האישי שלי בעבודה ב-SOC לאורך השנים, אני יכול לציין בבירור שעל מנת להשתלב טוב יותר עם הדרישות העסקיות של הארגון (בעיקר ארגונים גדולים), חשוב להטמיע תהליכי ממוכנים, ואוטומציה של תהליכי התגובה וניהול אירועים.

ישנן חברות שמתמחות ביישום מערכות ותהליכים ממוכנים לצורך אוטומציה של כלל או חלק גדול מהפעילות של ה-SOC, ואני ממליץ בחום לכל ארגון, בייחוד לארגונים הגדולים לאמץ מערכת כזאת.



NIST עובדים על טיוטת מסמך להמלצות

כיצד לאבטחת את ה-IoT

> עם הכח להשפיע באופן משמעותי כמעט בכל ההיבטים של החברה המודרנית, אימוץ הטכנולוגיה של האינטרנט של הדברים, או ה-IoT (Internet of Things) חושף אותנו לגל איומי סייבר שמהווה גם איום משמעותי על האומה.

הטיוטה הראשונה של המסמך שנקרא בשם Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) מתיימר לסייע לגורמים הרלוונטיים אשר מגדירים את המדיניות שימוש בציוד IoT, ואת ארגוני התקינה לפתח ולגבש סטנדרט אחיד למרכיבי IoT, מערכות ושירותים.

כדי לדחוף לכיוון סטנדרטיזציה בעולם ה-IoT NIST מעמידים מספר עקרונות:

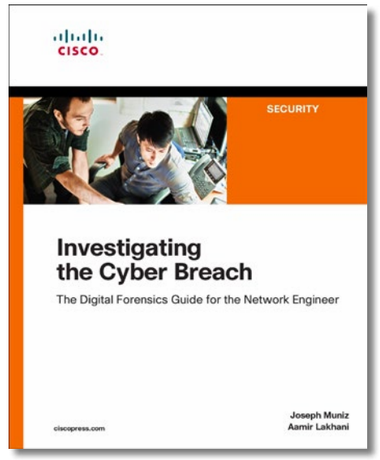
- הגדרת IoT כמושג המבוסס על רכיבים שונים בעלי אינטראקציה עם העולם הפיזי ובעלי יכולת אחסון נתונים, יכולת להתחבר לרשתות תקשורת, עיבוד ויכולת חישה.
- הגדרת יישומי IoT בעולמות תוכן מייצגים כגון ענף התחבורה, הצרכנות (כגון בית חכם), הבריאות (מכשירים רפואיים), מבנים חכמים וייצור חכם.
- סיכום ומיפוי תחומי הליבה של הגנת הסייבר בעולם ה-IoT כגון הצפנה, חתימה דיגיטלית, אבטחת חומרה, זיהוי ואימות, בקרת גישה, אבטחת הרשת, אוטומציית אבטחה וניטור רציף, ניהול שרשרת האספקה.
- הגדרת מטרות האבטחה של התקני ה-IoT, סיכונים, ואיומי הייחוס בהתייחס ליישומים הרלוונטיים.
- ניתוח שטח התקיפה לתחום ה-IoT, תוך התייחסות למרכיבים העיקריים של הטכנולוגיה.
- הצגת מטריצה של הסטנדרטים העיקריים לתחום אבטחת רכיבי IoT וכיצד הם מפתחים את תחומי הליבה ואת היישומים.
- מיפוי רשימת פערים בתקנים אפשריים, כגון החלת הטכנולוגיה Blockchain כדי לאבטח את רכיבי ה-IoT והמלצות ושיטות למניעת הידבקות בנוזקות ברמת התוכנה והקושחה.

הנספחים במסמך כוללים הגדרות, טבלת היכולות של ה-IoT, וכן טבלאות נרחבות המשקפות את רמת הבשלות של אבטחת המידע עבור ההתקנים IoT.



INVESTIGATING THE CYBER BREACH

The Digital Forensics Guide for the Network Engineer, First Edition



מדובר בספר מעולה, מבית היוצר של חברת סיסקו. הכותבים הינם Joseph Muniz המוכר והידוע, ו-Aamir Lkhani. הספר התפרסם בפברואר 2018, וניתן לרכוש אותו ברשת (אמזון).

הספר מכיל 13 פרקים, ומתמקד בעיקר בתהליך תגובה וניהול אירועים אבטחת מידע, לרבות תחקור דיגיטלי (Digital Forensics).

פרק 1:

תחקור דיגיטלי

הפרק דן בסוגיות של מה זה תחקור דיגיטלי, מהם השירותים של תחקור דיגיטלי, תהליך דיווח פשעי סייבר לשלטונות החוק השונים, חוקים ורגולציות בעולם של תחקור דיגיטלי, תפקידים ואחריות בתהליך תחקור דיגיטלי, סקר שוק של שירותי תחקור דיגיטלי, וכמובן מספק סקירה כללית על עולם ההכשרות המקצועיות בתחום התחקור הדיגיטלי.

פרק 2:

פשעי סייבר ודרכי התמודדות

הפרק מספק סקירה כללית על סוגי פשיעת סייבר, ודרכי התמודדות. כמו כן, הפרק נותן גם סקירה כללית של חוקים ותקנות בתחום פשעי הסייבר.

פרק 3:

הקמת מעבדת תחקור דיגיטלי

הפרק דן בסוגיות של הקמת מעבדה לתחקור דיגיטלי, כולל חומרה, תוכנה, ציוד ייחודי וכדומה.

פרק 4:

תגובה לאירועי סייבר

הפרק דן בסוגיות ההכנה ותהליכי התגובה לאירועי סייבר, לרבות אירועים בהם דלף מידע רגיש מחוץ לארגון. הפרק מספק הנחיות לבניית (Incident Response Plan (IRP, קביעת הגדרות לאירועי סייבר שונים, בהתאם לרמת החומרה של האירועים, וכדומה.

פרק 5:

תחקור אירועים

הפרק הזה דן בסוגיות של תחקור אירועי סייבר שונים, החל משלב הזיהוי, ועד לשלב סגירת האירוע.

פרק 6:

איסוף ושימור ראיות דיגיטליות

הפרק הזה דן בכל הסוגיות של תהליך איסוף ושימור הראיות הדיגיטליות במהלך תחקור אירוע סייבר. הפרק מספק סקירה מלאה על ציוד חומרה, ותוכנה שנדרש לטובת התהליך הזה.

פרק 7:

תחקור דיגיטלי בתחנות הקצה

הפרק הזה דן בסוגיות של ביצוע תחקור דיגיטלי ברמת תחנות הקצה, כגון מערכת הפעלה, קבצים, Registry, דפדפנים, תוכנות וכדומה.

פרק 8:

תחקור דיגיטלי ברמת הרשת

הפרק הזה דן בסוגיות של ביצוע תחקור דיגיטלי ברמת הרשת, באמצעות כלים ייעודיים כגון מערכות ניטור וניתוח לוגים (SIEM), Sniffers, מערכות IPS, Sandbox, מלכודות דבש (Honeypot) ועוד.

פרק 9:

תחקור דיגיטלי למובייל

הפרק הזה דן בכל הסוגיות של ביצוע תחקור דיגיטלי להתקנים ניידים (מובייל). הפרק מספק סקירה מלאה לסוגים השונים של מערכות ההפעלה של המובייל, וכיצד ניתן להוציא משם מידע חיוני לטובת החקירה.

פרק 10:

תחקור דיגיטלי של מערכות דוא"ל ורשתות חברתיות

הפרק הזה דן בסוגיות של ביצוע תחקור דיגיטלי במערכות דוא"ל, וברשתות החברתיות. הפרק מציג שיטות שונות לאיסוף וניתוח מידע מתוך מערכות דוא"ל, והרשתות החברתיות השונות.

פרק 11:

יכולות תחקור דיגיטלי של CISCO

הפרק הזה דן במערכות הייחודיות של חברת CISCO והיכולות שלהן מבחינת ביצוע תחקור דיגיטלי. הפרק מספק סקירה כללית של מגוון כלים ומערכות של CISCO, כגון: Ciscto Firepower, Cisco Advanced Malware Protection (AMP), Meraki, Cisco Stealthwatch, Cisco Cloudlock, Cisco Umbrella ועוד.

פרק 12:

ניתוח מקרים של תחקור דיגיטלי

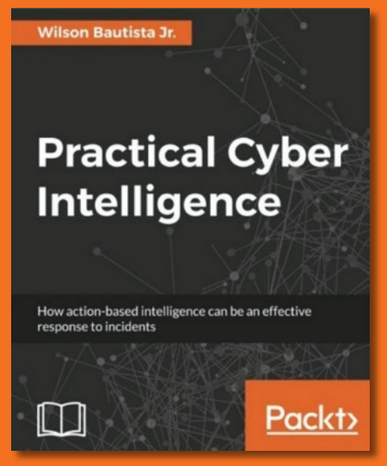
הפרק הזה דן בסוגיות של ניתוח מקרים של תחקור דיגיטלי, הן ברמת תחנות קצה, ברמת הרשת, תחקור נוזקה, תחקור התקני מובייל, ותהליך כללי של תחקור אירועי סייבר.

פרק 13:

כלים ייעודיים לתחקור דיגיטלי

הפרק הזה מספק סקירה כללית על מגוון עשיר של כלים ייעודיים (מבוססים קוד פתוח ומסחריים) לביצוע תחקור דיגיטלי ברמות שונות (ברמת התחנה, ברמת הרשת, על התקנים מובייל, על נוזקות ועוד).

PRACTICAL CYBER INTELLIGENCE



הספר נכתב ע"י Wilson Bautista, ופורסם במרץ 2018. הספר מכיל 15 פרקים, שמתייחסים לכל עולמות התוכן של שירותי מודיעין סייבר.

פרק 1:

הצורך בשירותי מודיעין סייבר

הפרק הראשון מדבר על הצורך בשירותי מודיעין סייבר, סוגי שירותי סייבר, שיטות לאיסוף נתונים, ועוד.

פרק 2:

פיתוח יכולות מודיעין

הפרק דן בתהליך פיתוח יכולות מודיעין בתחום הסייבר, החל מהירכיה של תהליך איסוף המידע, ועד למחזור חיים של מודיעין ומידע.

פרק 3:

אינטגרציה בין מודיעיין סייבר ותפעול מערך אבטחת המידע

הפרק הזה דן באינטגרציה בין שירותי מודיעין הסייבר לבין תפעול וניהול מערך אבטחת המידע בארגון. הפרק מציג מבט אחר על תהליך תפעול מערך אבטחת המידע, ומספק הנחיות לגיבוש אסטרטגיה לבניית יכולות מודיעיניות. הפרק גם דן בבעלי התפקידים והאחריות שלהם מבחינת שירותי מודיעין.

פרק 4:

שימוש במודיעין סייבר למימוש מעטפת הגנה אקטיבית

הפרק הזה דן ביכולות השימוש בשירותי מודיעין סייבר למימוש אפקטיבי של מעטפת הגנה אקטיבית מפני מתקפות סייבר. מציג מודלים להגנה אקטיבית, מספק תובנות אודות ה-Cyber Kill Chain, ואימוץ שיטות שונות למימוש הגנה אקטיבית בארגון.

פרק 5:

עקרון ה-F3EAD

הפרק הזה מציג את העקרון שימוש ב-F3EAD (ר"ת של Find, Fix, Finish, Exploit, Analyze and Disseminate), עקרון שמקורו במערכי מודיעין צבאי. הפרק מסביר את העקרון, את תהליכי העבודה עפ"י העקרון הזה, כיצד עושים בו שימוש בארגונים ממגזרים שונים (מסחרי, ממשלתי, בטחוני וכו').

פרק 6:

אינטגרציה בין מודיעין על איומים לבין תפעול אבטחת המידע

הפרק הזה דן בסוגיות שונות של שירותי מודיעין ייחודיים שמתמקדים באיתור איומים (מגמות לאחור ותחזית לעתיד), מסביר את העקרונות של שירותי המודיעין לאיתור איומים פוטנציאליים, ומציג גם תפיסה של מודל בשלות של תהליך מודיעין על איומים.

פרק 7:

יצירת מסגרת לשיתוף פעולה

הפרק הזה דן בצורך בבניית מסגרת לשיתופי פעולה עם גופים שונים (ממשלתיים ומסחריים), מציג את המטרות, אסטרטגיה, ודרכי פעולה בהיבט האסטרטגי, הטקטי והאופרטיבי.

פרק 8:

מעטפת ההגנה על הארגון

הפרק הזה מציג את מערך אבטחת המידע בארגון, כגון מרכז לניהול אירועי אבטחת מידע (SOC), את השירותים השונים שה-SOC מספק לארגון, בקרות תפעוליות שונות כגון ניהול תצורה, ניהול טלאים ועוד.

פרק 9:

הובלת שירותי מודיעין סייבר

הפרק הזה דן בסוגיות של ניהול שוטף של שירותי מודיעין סייבר, בחסרונות, ביתרונות, ובמודעות של הנהלות הארגונים לשירות מסוג זה.

פרק 10:

ניהול תצורה וזיהוי אנומליה

הפרק הזה דן בסוגיות של הגדרת ניהול תצורה למערכות השונות, וזיהוי אנומליה ברמת המערכות ו\או הרשת. הפרק מציג סוגיות שונות של אתגרים בניטור ואיתור אנומליה.

פרק 11:

כיבוי שריפות

הפרק הזה דן בסוגיות של תגובה לאירועי אבטחת מידע, ומציג סוגיות שונות של התמודדות עם אירועים עפ"י תרחישים שונים (אירועי סייבר שונים).

פרק 12:

הערכת וניהול פגיעויות

הפרק הזה דן בסוגיות של הערכת וניהול פגיעויות (Vulnerability Management). הפרק מציג את התפיסות השונות כגון CVE ו-CVS, ושיטות שונות לביצוע סריקות וניהול פגיעויות, כולל התייסות למחזור החיים של הפגיעויות, תוכניות הפחתה ודיווח לגורמים הרלוונטיים.

פרק 13:

הגדרת רמות סיכון

הפרק הזה דן בסוגיות ניהול והערכת סיכונים בהיבט העסקי, ומציג רמות סיכון שונות, בהתאם לפעילות העסקית של הארגון.

פרק 14:

מדדים

הפרק הזה דן בסוגיות של הגדרת מדדים (KPI), ומדידת האפקטיביות של שירותי המודיעין, ומערך אבטחת המידע בארגון.

פרק 15:

סיכום והפקת לקחים

הפרק הזה די מסכם את כל הספר במבט מלמעלה.

10 שלבים לביצוע מבדק חוסן מוצלח



מאת: **אלן הרשקו**,
מנהל אבטחת המידע
של חברת NEOGAMES

בעולם התקינה והרגולציה ישנם לא מעט סטנדרטים ומסגרות שמספקות המלצות והנחיות כיצד לנהל אבטחת תחום אבטחת המידע בארגון. אך זה לא די בכך, ועל הארגון לנקוט באמצעים נוספים על מנת לבחון את רמת אבטחת המידע של הארגון ומערך המחשוב שלו. אחת מהדרכים האפקטיביות ביותר לבחון את רמת הבשלות של מערך המחשוב בארגון הוא באמצעות בדיקות חוסן.

ביצוע בדיקות חוסן בצורה נאותה, דורש ידע, ניסיון, שימוש בכלים ושיטות או מתודולוגיות מקובלות. לפניכם 10 טיפים לביצוע מבדקי חוסן בצורה נאותה:

טיפ 1: סוג ושיטות הבדיקה

על מנת לבחון את רמת הבשלות של הארגון ומערך המחשוב שלו, יש צורך בתיחום נכון של מבדק החוסן. מרבית הארגונים בוחרים לבצע בדיקת חוסן מבחוץ, או בדיקת חוסן למערכת מסוימת, ולא לבחון את כלל מערך המחשוב של הארגון.

בדיקת חוסן אפקטיבית הינה בדיקה מקיפה יותר, שכוללת את כלל מערכות המחשוב שנמצאות בתוך תיחום הפרויקט. בדיקה זו תכלול ביצוע ניסיונות תקיפה מתוך הרשת הארגונים ומבחוץ (כדי לדמות דרכי פעולה של תוקף אמיתי). ישנם מספר סוגים ושיטות בדיקות חוסן שמקובלות בעולם, כגון בדיקות חוסן בשיטת Black Box, White Box ו-Gray Box.

הסוג הראשון של בדיקות החוסן הינו ה-Black Box. מדובר בסוג בדיקה שמדמה מתקפה של תוקף אמיתי (האקר). בסוג בדיקה זו, התוקף (חברת הייעוץ שנשכרה לבצע את הבדיקה), אינו יודע כלום על הארגון, ועליו לבצע בדיקת חוסן במטרה להצליח לפרוץ לארגון בכל דרך אפשרית (בהתאם לתיחום וסוג הבדיקות והכלים שאושרו במסגרת ה-SOW).

לסוג בדיקה זו, ישנה 2 אפשרויות: אפשרות אחת הינה ביצוע מבדק בשיטת Blind – כלומר, התוקף אינו יודע שום דבר על המטרה (על הארגון שנבדק). האפשרות השנייה הינה בשיטת Double Blind – כלומר, התוקף אינו יודע כלום על הארגון הנבדק, אבל גם צוות אבטחת המידע בארגון אינו יודע כלום על הבדיקה, כלומר זה מתבצע בהפתעה גמורה מבחינתם. בדיקה זו בד"כ מתוזמנת ע"י ההנהלה, או המבקר פנים בארגון, ולעתים ע"י רגולטורים ו\או חברות צד ג' נוספות כגון הלקוחות (שמבחינתם הם מבצעים בדיקת אבטחה על הספק שלהם, כחל מתהליך ניהול סיכונים בשרשרת האספקה).

המטרה העיקרית של בדיקה זו, הינה לבחון גם את האפקטיביות של צוותי התגובה בארגון, ולא רק את החוסן של הרשת ומערכות המידע.

הסוג השני של הבדיקה הינו White Box. בבדיקה זו, התוקף כן יודע נתונים אודות הארגון, ואף לפעמים מקבל מידע או נתונים נוספים כגון חשבון משתמש במערכת, אמצעי זיהוי ואימות חזקים (2FA), שרטוט רשת, סקירת ארכיטקטורת של היישומים והרשת ועוד. לעתים, בדיקה זו גם כוללת סקירת קוד (ידני או אוטומטי באמצעות כלים ייעודיים לכך).

הסוג השלישי של הבדיקה הינו Gray Box, שזה שילוב של שתי השיטות יחד.



טיפ 2: תיחום הבדיקה

בתיחום הבדיקה, נכללים מגוון פרמטרים כגון איזה מערכות בודקים, אם יש כמות גדולה של מערכות – אזי איזה מדגם לוקחים, טווחי כתובות IP, אם נכללות גם בדיקות פישינג – אז האם זה על כלל עובדי הארגון, או רק צוותים שונים (Spear Phishing), או אפילו רק מיוחד להנהלה (Whale Phishing), איזה כלים מותר לעשות שימוש במסגרת הבדיקה, ועוד.

טיפ 3: תכנון נכון של מבדק החוסן

עליכם להתייחס למבדק חוסן כמו אל כל פרויקט. מצד הארגון, עליכם להשיג אישור הנהלה ומשאבים (כסף וכח אדם) לביצוע המבדק. עליכם לבחון מספר ספקים מבחינת היכולות שלהם, ניסיון עם המערכות ומבנה הארגון או של תשתית המחשוב שנמצא אצלכם בארגון, ולתכנן היטב את המבדק.

טיפ 4: מסגרת זמן

לעתים, הארגון נדרש לבצע בדיקות חוסן כחלק מדרישות הלימה לתקינה מסוימת, או רגולציות ואף דרישות לקוח. עליכם לוודא שמסגרת הזמן שמוקצית לביצוע המבדקים, כולל בדיקה חוזרת לאחר תיקון הממצאים, הולמת לדרישות החוקיות, רגולציה, וחוזיות – מבחינת מסגרת הזמן. תקחו בחשבון, שאם יימצאו ממצאים בעלי רמת חומרה גבוהה, על הארגון לתקן את הממצאים בטרם ביצוע הבדיקה החוזרת, מה שעלול לקחת זמן נוסף, שעלול לגרום לכם לחרוג מתוך מסגרת הזמן שהוקצתה לכך.

חשוב גם ליישק קן עם החברה הסוקרת, מבחינת תיחום, סוג הבדיקה, ציר הזמן, וכמות האנשים שיעבדו לצורך עמידה בזמנים. תשימו לב גם לדרישות של הצוות הסוקר. אם יימסר מידע שגוי (כגון כתובות IP לא נכונות או שיחסרו כתובות IP מהתיחום של הבדיקה) זה עלול לגרום לחריגה במסגרת הזמן.

טיפ 5: תקשורת ודיווח על תוצאות הבדיקה

בזמן הבדיקה, יתכן ויימצאו ממצאים בעלי רמת חומרה גבוהה מאוד. לא צריך לחכות עד לסיום הבדיקה על מנת לדווח על הממצאים הללו, היות והתוקפים (האמיתיים) כבר מודעים גם כן לחולשות, ומנסים או ניסו לתקוף את מערך המחשוב של הארגון. חשוב לקבוע מראש על דרך התקשרות ודיווח (למי מדווחים) במקרים כאלו. היות והמידע רגיש ביותר, זה לא יישלח במייל רגיל, אלא בתווך מוצפן כלשהו.

טיפ 6: חשיבה מחוץ לקופסה

בעת תכנון הבדיקות, חשוב לחשוב מחוץ לקופסה. תנסו להריץ תרחישים שונים בסגנון של "מה אם" (What If), ותבססו את התיחום של הבדיקות על התרחישים הללו. יתכן והצוות הסוקר יחשבו על תרחישים שונים (נוספים) לצורך הבדיקה. היו פתוחים, ותנתחו ביחד את התרחישים ותבחרו את הדרכים הטובות ביותר לבחון את רמת אבטחת המידע של הארגון.

אחד ההבדלים בין סריקת וניהול פגיעויות (Vulnerability Assessment and Management) לבין מבדקי חסון, הוא שבמבדקי חסון בוחנים תרחישים שונים בפועל, ולא בתיאוריה (של מה היה קורה אילו .....). מטרת הבדיקות הללו הינן לאתר חולשות ולבחון האם ניתן לנצל אותן כך שהתוקף יצליח להשיג את מטרות הבדיקה (פריצה והשתלטות, גניבת מידע רגיש וכו').

טיפ 7: תוכנית ניטור ומעקב

חשוב לתכנן תוכנית ניטור ומעקב במשך תקופת הבדיקה. היות והמטרה של הבדיקה היא לבחון את היכולת של המערכות לזהות מתקפות ולהתריע, זהו זמן טוב לבחון את האפקטיביות של המערכות מבחינת זיהוי התקיפה. כמו כן, זה יאפשר לבחון גם את הכשירות של צוותי התגובה בארגון.

חשוב שהבקרים ואנליסטים ב-SOC יתעדו את כל האירועים במסדרת הזמן שבה בוצע הבדיקה, לצורך הפקת לקחים. תהליך חכם של תיעוד נכון והפקת לקחים, יכול לסייע בחיזוק שרשרת האבטחה באמצעות טיוב מערכות ותהליכי עבודה בארגון, לרבות ה-Incident) IRP Response Plan).

טיפ 8: דו"ח הבדיקה

חשוב לבקש מהספקים שני דוחות: דוח אחד מתומצת – להנהלה (עדיף בליווי מצגת הנהלה עם עיקרי הממצאים, ותוכנית טיפול בממצאים, כולל משאבים ונתונים נוספים כגון - האם הטיפול בליקויים פוגע ב-TTM ואם כן, בכמה).

הדוח השני מיועד לצוותים הטכנולוגיים (IT ו-DevOps או פיתוח). הדוח הזה מפורט יותר, ומטרתו הינה לספק כמה שיותר מידע אודות הממצאים (ממצא, כיצד נמצא, איפה נמצא, מידת הנזק על המערכת או פעילות עסקית, מהי רמת הסיכון, המלצות לסגירת החולשות ועוד).

טיפ 9: הפקת לקחים

תהליך הפקת לקחים הינו תהליך מאוד חשוב בכל פעילות ולא רק במבדקי חוסן. אבל בייחוד, כאשר מדובר על מבדקי חוסן, תהליך הפקת לקחים מקבל משקל גבוה יותר. מטרת תהליך זה הינו לבחון את הפקטיביות של הצוות התגובה לאירועים, וגם לשפר את מערך אבטחת המידע בהתאם לממצאים שעלו במבדק. זה יכול לכלול שינויים בהגדרות (כגון ניהול תצורה, הקשחות, טלאים, שינוי ארכיטקטורה), הוספת פתרונות אבטחת מידע חדשים או טיוב פתרונות קיימים, שינוי תהליכי עבודה וכתיבת נהלים והטמעתם בארגון, עדכון מסמך ה-IRP, ועוד.

ניתן להגדיר מדדים (KPI) לפני הבדיקה, ולמדוד אותם לאחר הבדיקה לצורך בחינת תהליך שיפור מתמיד (באם קיים), ואם לא, אז איפה טעינו ומה ניתן לשפר. ה-KPI יכולים לנוע בין כמות ממצאים ברמת חומרה שונים, לבין זמן שלוקח לטפל (סגירת הליקויים), זמני תגובה לזיהוי האירוע, ועוד.

טיפ 10: מעקב טיפול בממצאים

לאחר שהמבדק הסתיים, עבודתו של ה-CISO טרם הסתיימה. על ה-CISO להכין תוכנית מערב לטיפול אחרי הממצאים, כפי שעלה בסקר. התוכנית צריכה להתייחס לפרמטרים כגון הממצאים (סוג וכמות), אחריות ביצוע לתיקון הליקוי, תאריך יעד (עד מתי זה יתוקן), מנהל סיכון של מערכת או מערך תשתיתי , ועוד.

לפעמים, לאחר סיום מבדק חוסן, הארגון לוקח הפוגה קצרה על מנת לתקן את הממצאים, ואז מבקשים מהספק לבצע בדיקה חוזרת. במקרה כזה, חשוב באמת לוודא שכל הליקויים נסגרו (לפחות אלו ברמת קריטיות גבוהה).

הכירו את ה-CLOUD ACT
וכיצד ניתן להתגונן מפניו?

חוק הגנת הפרטיות ספג מהלומה חזקה, כאשר ה-Cloud Act אושר בקונגרס האמריקאי,במרץ 2018. לא התקיימה הצבעה בנושא, אלא הצעת החוק שולבה בין מסמך דרישות של 2,232 עמודים, ועם בקשת תקציב של 1.3 טריליון דולרים.

הצעת החוק משנה את האופן שבו גופי ממשל יכולים לקבל גישה למידע שלנו. זה מספק לממשל האמריקאי ולממשלות זרות את האפשרות לבקש גישה למידע ללא צו בית משפט.

אז מה זה בעצם ה-Cloud Act?

הכל החל לפני מספר שנים, במהלך חקירה פלילית שבה היה מעורב תושב אירלנד. הממשל האמריקאי השיג צו בית משפט וביקשה מחברת מיקרוסופט גישה לחוות השרתים שממוקמת באירלנד. מיקרוסופט סירבה למסור את המידע, בטענה שהשרתים אינם ממוקמים בשטח ארה"ב, ולכן אין שום הצדקה לכבד את דרישות צו בית המשפט האמריקאי. התיק נגרר 4 שנים.

וכיום, לאחר שהצעת החוק אושר, תחת ה-Cloud Act, הממשל האמריקאי אינו צריך צו בית משפט על מנת לקבל גישה למידע שמאוחסן באירופה. כעת, למיקרוסופט אין ברירה אלא להיענות לבקשת הממשל האמריקאי, ולמסור את המידע המבוקש. ישנם שתי הוראות עיקריות בתוך הצעת החוק של ה-Cloud Act:

- **עקרון ראשון**: מאפשר לספק גישה לכל ישות אכיפת חוק, החל ממשטרה מקומית, ועד לגופים פדראלים, כדי לגשת לתוכן דיגיטלי שמועבר בתקשורת ו\או לכל רשומה אחרת, ללא קשר למקום שבו מאוחסנים הנתונים. בתנאי שהחברה ממוקמת בארה"ב, הם ייאלצו למסור את הנתונים, גם אם השרת נמצא במדינה זרה.
- **עקרון שני**: מאפשר לנשיא ארה"ב לרקום "הסכמים מנהליים" עם מדינות אחרות, שיאפשרו להם גישה לנתונים שמאוחסנים מחוץ לארה"ב, ללא שום צו בית משפט. לאחר מכן, ניתן יהיה להשתמש במידע זה על מנת להרשיע אזרחי ארה"ב, למרות שהמידע שהושג, נאסף ללא צו בית משפט.

החוק החדש די מפחיד את כלל אזרחי ארה"ב, ומביא מהלומה חזקה לחוקי הגנת הפרטיות.

תחשבו על מקרה זבו ממשלה זרה חוקרת את אחד מאזרחיה, ומבקש לקבל גישה לרשתות החברתיות שלו, כגון פייסבוק. פייסבוק יהיו מחוייבים למסור את כל המידע, ללא צו בית משפט, וזה עלול לכלול מידע על אזרחי ארה"ב.

והפוך, ממשלות זרות, יהיו מסוגלות למסור חופשי מידע שמאוחסן באירופה למשל, לממשל האמריקאי, וכל זה ללא שום צו בית משפט.

ניתן לקרוא אודות החוק החדש בקישור הבא: Cloud Act. (תגלגלו לעמוד 2,201).

אז מה ניתן לעשות על מנת לשמור על הפרטיות שלנו?

אומנם זה יישמע קיצוני, אבל אם תרצו עדיין לשמור על הפרטיות שלכם...להלן כמה עיצות והמלצות למימוש:

1.השתמשו תמיד בשירותי VPN

תרכשו חשבון באחד משירותי ה-VPN ברשת האינטרנט, מה שיאפשר לכם לשמור על האנונימיות ברשת. חשוב לבחור ספקים שאינם מהווים חלק מה-Five Eyes Alliance, כגון ExprexVPN (שממוקם British Virgin Islands) או NordVPN (שממוקם ברומניה).

2.תמחקו את החשבון בפייסבוק

האמינות של פייסבוק נפגעה חזק לאחרונה, לאחר שפורסם שמעל 87 רשומות (חשבונות פייסבוק) שותפו לא כחוק עם גופים צד ג'. הרשתות החברתיות, ובייחוד פייסבוק, מהווה מכרת זהב עבור ממשלות וכוחות הביטחון, אשר מעוניינים למצוא מידע רגיש וקצת "לכלולך" על חשודים פוטנציאליים. מישהו מהמכרים, חברים, משפחה, עובדים, וכדומה, יכולים לפרסם משהו בפייסבוק אשר עלול לשמש נגדכם כראיה בחקירה בבית המשפט, ולכן זה הגיוני שגם כוחות הביטחון יראו לגשת למידע הזה. וכעת, עם הצעת החוק החדש של ה-Cloud Act, הגישה למידע תהיה קלה יותר. הפתרון הוא לנטוש את הענקית, ולמחוק את החשבון במיידית.

3. תמחקו את החשבון ב-Dropbox

מלבד העובדה שהחברה נפלה קורבן למספר מתקפות סייבר בשנים האחרונות, אירועים בהם גם דלף מידע רגיש החוצה של משתשמים, וכעת, עם הצעת החוק החדשה, הגישה לנתונים תהיה קלה עוד יותר.

אם הפרטיות חשובה לכם, ניתן לפתוח חשבון בחברת SpiderOak, שאושרה גם ע"י לא פחות ולא יותר אדוארד סנוודן. למרות שהשרתים נמצאים בארה"ב, החברה אינה מפחדת להתעמת עם הממשל, וגם עם יידרשו למסור את המידע, היחידים שיש להם את המפתח הפרטי לנתונים זה המשתמשים עצמם.

4. הימנעו מאחסון נתונים בענן

השימוש בענן משפר לנו את החיים מבחינת אחסון וגיבוש המידע, וגישה חופשית בכל זמן, ומכל מקום. החסרון הגדול הוא שכעת, בעקבות החוק החדש, יהיה אפשר לקבל גישה לכלל השרתים של החברה, ולצפות בכל המידע שמאוחסן עליהם, ללא צו בית משפט. אם אתם צריכים להשתמש בשירותי ענן, היעזרו בשירותים כגון Tresorit , שמשתמש בהצפנה מקצה לקצה, והשרתים אינם מאוחסנים בארה"ב, אלא במדינות שאינן חלק מה-Five Eyes Alliance. ואם אתם רוצים להגן על המחשבים האישיים שלכם, מומלץ להשתמש בתוכנית VeraCrypt.

5. החליפו את החשבון GMAIL שלכם ב-ProtonMail

תדמיינו לכם, שבגלל שקיבלתם מייל מחבר ישן, כותחות הביטחון יוכלו לגשת כעת לכל תיבת הדוא"ל שלכם, ולקרוא את כל המיילים. זה מה שקורה למי שמשתמש בשירותי של גוגל, Yahoo או כל השירותי דוא"ל האחרים שמקורם בארה"ב.

אם אתם צריכים להשתמש במייל חיצוני, היעזרו בפתרון של ProtonMail. השירות אנונימי לחלוטין, ולא נדרש שום מידע אישי לצורך הפקת חשבון דוא"ל. הם לא שומרים כתובות IP, והכל מוצפן מקצה לקצה. והדובדבן שבקצפת, היא שהשירות ממוקם בשוויץ, ומוגן ע"י החוקים הנוקשים של שוויץ. היוצרים של השירות הזה, יצרו גם שירותי ProtonVPN, שמתממשק עם TOR ומספק רמה גבוהה של אנונימיות.

6. הימנעו מחיפוש ב-Google

גוגל, ביחד עם מיקרוסופט, אפל, ופייסבור הם חלק מהתומכים הגדולים של החוק החדש, מה שאומר שהם יהיו יותר משמחים למסור את המידע שלכם, אם בקשה כזו תגיע למשרדיהם. ואנחנו יודעים שגוגל יודעת עלינו יותר דברים מאשר אנחנו יודעים על עצמנו..., הרי מי זוכר על מה עשינו חיפוש ערב אחד שהיינו שיכורים???!!! האם אנחנו רוצים שהמידע הזה יגיע לרשויות החוק?

אומנם גוגל הינו מנוע החיפוש הטוב בעולם, אבל יש לו חלופות, כמו למשל StartPage , שיניב לנו תוצאות חיפוש לא פחות טובות, אבל בטוח יותר מאובטחות מבחינת שמירת האנונימיות שלנו. הם לא שומרים שום מידע, ולכן אין להם גם מה למסור במידת ותגיע בקשה לכך.

משימה קשה, אך אפשרית

השמירה על הפרטיות שלנה נהייתה כמעט משימה בלתי אפשרית, אבל עם הרבה מאץ, נוכל עדיין לשמור על הפרטיות שלנו. אנחנו לא אומרים שצריך לרדת מתחת לרדאר ולהסתגר בחדר סגור, רק להיות זהירים יותר מבחינת איזה מידע אנחנו מוכנים לחלוק ברשת האינטרנט. מי יודע איך זה יתפוצץ לנו בפנים יום אחד...



לגרום לשטן לבכות

שלום חברים, חזרתם! מוכנים לשמוע על המשך ההרפתקאות של קררמפוס? ברוכים השבים! ולמי שמציץ בפעם הראשונה, הרשו לי להציג את עצמי, אני קררמפוס (Krrampus, לאלה ששאלו...) ואני שד אינטרנטי שובב שאוהב לצוד חוטאים ברחבי הרשת, אתן לכם שנייה לעכל וארחיב עם חיוך. איך אני צד? שמח ששאלתם, יש לפניכם הזדמנות מצוינת להבין זאת דרך הסיפור הבא, על אחד מסיורי הלילה האחרונים שלי. אז אתם מכירים את הנוהל... שבו בנחת, תרימו את האספרסו תתרווחו ותקשיבו.

כמיטב הדברים הטובים שקוראים לנו במהלך החיים, הרפתקה זו התחילה בשעות הקטנות של הלילה בעודי משוטט ברחבי מימדי הסייבר השונים, לפעמים אני נתקל בחדשות ה-Unicorn Post, או בוהה שעות בסרטונים ב-YouTard וסתם לחפש צרות על ה... קרניים שלי. ומשהו קורץ לי בקצה של העין, אתר ממש מוזר, "Heaven20.com" (גילויו נאות – עכשיו רק בינינו... ביקרתי באתר הזה כבר, או בגרסה קודמת שלו. לא התחברתי: הכול בצבע לבן מסנוור, מוזיקה מרגיעה שאני לא יכול לסבול, חדי קרן בכל מקום, ואיזה גבר עם שיער ארוך לבוש בשמיכה שיש לו סטייה מוזרה למיין דברים בלי הפסקה - לא מפסיק לשלוח אנשים ימינה ושמאלה... יצאתי משם במהרה לפני שאקבל אלרגיה) מעניין איך זה נראה עכשיו, קליק על הקישור ונפתח באנר ענקי שיורק לכיווני את כל המילים הטרנדיות הקיימות : "הדבר הBig Data בגן עדן!", "בלתי ניתן Cyber למתחם שלנו!", "מבטיחים שביעות Integrity של כלל היצורים!", חייב לציין שאיפשהו כבר שמעתי סיילס פיצ' מאוד דומה... בוא נלך לראות מה זה.

קליק קדימה קליק אחורה, סרטון פרומו בקישור הזה, ועוד חלון קצר בגוגל וכלי אחד או שניים לדוגמת theHarvester אני מוצא עשרות פרופילים שונים ברשתות חברתיות, רגע למה? מפעיל חיפוש ב whois, הפנייה לאותה הכתובת המיילית המדוברת ועוד כמה עשרות קישורים לאתרי הונאה. עוצר לסדר את המחשבות רגע, זה כבר דורש אופרציה – מתי הבחור מספיק לישון? מעניין אם הוא מנהל הכול במערכת מרכזית, מחשבה לעתיד, רושם בפנקס לאחר כך.

הגיע הזמן להפשיל שרוולים ולמצוא את הטרול האחראי לכל זה! עוברים על כל פירור, מה יש לנו פה: כינוי the_satan זהו? הבחור זהיר, טוב חופרים יותר עמוק. רגע, מה אני רואה פה? בינגו! איזה בחור Stan Hellbjorn מופיע באתר הכרויות שוודי בשם Skol. היתכן? וידוי קטן של כתובת המייל מאמת את זה! נראה כמשתמש פעיל, השאיר שם המון פרטים וכולם אישיים... כמה הוא אוהב את ההורים שלו, את סבתא, את סבא, בקיצור הבנתם, Cambridge Analytica פשוט מתים עליו.

הודעה מ-nmap הופיע על המסך פורט 666 פתוח, מנסה לגשת באמצעות דפדפן אבל מקבל תשובת Illegal Request, מעניין, ומה יקרה עם ננסה לגשת באמצעות ncat והופה קופץ לו באנר על כל מרחב הקונסול שלי, Welcome to Hell! (פלאשבאק, שתייה לא משהו והבנות כולן עם זקן תיש, לא שאני נגד, פשוט אני לא חובב גילוי עריות). משפשף את העיניים, מה זה היה בדיוק? אני חושב שיש לי גישה לשרת... מכאן הוא בטח מנהל את כל האופרציה וההונאות. קררמפוס, רגע, לא לחגוג מוקדם מידי, בוא נראה אם אני מצליח להיכנס פנימה... כמו שפחדתי יש שם משתמש וסיסמה, שיט! שעת יצירה, גייסתי את כל היצירתיות שלי אבל זה כשל. ומשהו אומר לי שגם כלי אוטומטי לא היה הולך פה, כן, הגבלה לחמש ניסיונות כושלים. טוב חושבים על תכנית חלופית.

אתם זוכרים שבהרפתקה הקודמת, כשפרצתי אתר פורנו, החלפתי את חוקי הדואר הנכנס כך שאני אקבל את כל הדואר הכועס של המשתמשים, מעניין אם קיבלתי דואר כועס מ Stan- שלנו? מריץ חיפוש - ומה אתם יודעים? מסתבר ש-Stan היה מבקר קבוע, אני מתחיל לקרוא את המייל וסימפוניה של כעס ותסכול מתנגנת לאוזני. כמה שאני נהנה לקרוא דואר מעריצים. אחריי כמה דקות, לפיד נדלק לי בין הקרניים, ונופל לי האסימון שיש לי ביד ערוץ תקשורת פתוח מול Stan. אולי אני פשוט אשלח לו מייל "פיצוי" עם קצת קצפת בצורת meterpreter קליק אחד ויש לי גישה למחשב שלו! קררמפוס, אני בדרך כלל לא מחמיא לך, אבל הפעם יצאת שד ממזר לא קטן. לאחר הכנה של הפיילוד, בחרתי ב-stageless, בלי צורך במשיכה של פונקציונליות לאחר הרצה ראשונית, הכנתי את מייל ה"פיצוי" בצורה של שובר מתנה פיקטיבי להופעה של להקת kpop האהובה עליו. הרי כל מה שצריך זה להשתמש באובייקט DDE שמריץ פקודת powershell על התחנה. בפועל מוריד את הפיילוד משרת שנמצע בבעלותי, וכל זה מתחת לרדאר ובלי להדליק נורה אדומה באנטי-וירוס!

הקובץ חם, התשתית רצה. מייל הפיצוי המכיל את ההתנצלות מכל האפס לבבות שלי, נכתב. מוזיקת מטאל מחרישת קרניים מרעידה את הרקע ואני לוחץ "שלח" בתקווה ש-Stan שלנו יפתח את המסמך בהקדם. לאחר שעה של המתנה שהרגישה לי כמו נצח נצחים, אפילו בממדים של שדים קיברנטיים. מופיע המשפט המיוחל מכל בטרמינל: "Opened 1 Meterpreter Session". עכשיו אפשר להתחיל לחגוג, שלום לך אדון Stan בוא נראה מה אתה מסתיר בחדרים החשוכים שלך. unicorn_pron בתיקיה אקראית, לא זה לא זה, hello_kitty_tottaly_not_pron, לא מעניין, zuckerberg_and_equifax, נו באמת חבר, איפה פרטי הגישה? סיסמאות? רגע, מה זה: תיקייה בשם hell_project וכמובן שהכול פה, פרטי התחברות לתשתית, פרטים של האנשים שנפלו בפח, כל המטעמים שיש בגיהינום.

עכשיו חבר כשאתה אצלי בכיס, נותר להחליט מה עושים עם כל האופרציה שלך. פשוט להוריד אותה זה לא מספיק משעשע ופומבי, האצבעות מתחילות לרוץ לפני שהמוח מספיק להבין מה אני עושה, קישור לפה, הדבקה שם, הפניה והנה עכשיו כל האתרים שלו מפנים לפרופיל שלו באתר ההיכרויות השוודי, כדי שכולם ידעו איזה מעריץ גדול הוא של להקות kpop, וכמה אוהב את אמא ואבא... ומה עושם עם כל הכסף שהוא צבר מההונאות, קליק קלאק וכל הכסף נתרם לעמותה של אחי השד -בפומט, הוא בדיוק פתח איזה מסדר של איזה בחור בשם שלמה... זה בטוח יגרום ל-Stan שלנו לדמוע מרוב אושר. ואגב, התשובה היא 42.


היי, מתי?
אני לא יודעת. אולי בעוד שבוע?
אני לא יודעת מה לומר.
אני לא יודעת מה לומר.
אני לא יודעת מה לומר.



קבוצת טיטנס סקיוריטי מציגה

CERTIFIED CISO

כולל הכנה להסמכת CISM הבינלאומית מטעם ארגון ISACA

משך הקורס: 200 שעות אקדמיות

קבוצת Titans Security חיברה את הקורס המוביל בישראל להקניית כלי הניהול המתקדמים ביותר עבור מנהל אבטחת המידע, על בסיס הניסיון המצטבר של סגל המרצים הבכיר של החברה, הן בצד האקדמי והן בצד הפרקטי.

בכדי שנוכל להקנות למשתתפי הקורס את הכישורים להבין את התמונה הכוללת והרחבה של תפקיד מנהל אבטחת המידע ואת היכולות לחזות את הסיכונים והכשלים העומדים בדרך להצלחה. ניתן דגש מיוחד לניתוח אירועים ודיונים בין משתתפי הקורס ומנחיו על בסיס Case Studies של אירועים אמיתיים בארגונים שונים בארץ ובחו"ל.

זהו המסלול היחיד שכולל הכנה מלאה לבחינות ההסמכה בפורמט החדש (100% הצלחה בבחינות האחרונות) כי אין מנהל אבטחת מידע לא מוצלח, יש מנהל אבטחת מידע לא מודרך!

למה כדאי ללמוד אצלנו?

- הצלחה בטוחה למעלה מ-98% הצלחה בבחינות הגמר
- מיטב המרצים בתעשייה הישראלית והבינלאומית
- תרגול מעשי רב ומגוון בנושאים העכשוויים
- Networking עם מיטב הבכירים במשק הישראלי
- חברות שנתית באיגוד העולמי לאבטחת מידע ISSA ובאיגוד הישראלי
- מלגות והטבות ייחודיות לחיילים משוחררים וסטודנטים
- ערכות לימוד ייחודיות ובלעדיות

והדבר הכי חשוב, היות ואנו בטוחים בהצלחה שלנו, אנו מציעים לכלל התלמידים הטבות נוספות:

לא עברת את הבחינה?
קבל קורס חוזר ב-50%
(ללא אותיות קטנות)

עברת את הבחינה?
קבל זיכוי של עלות הבחינה,
לניצול בקורס הבא במכללת Titans security

למידע נוסף וקביעת פגישת ייעוץ:
טלפון: 077-5150340 | info@titans2.com

TSA Titans Security Academy

TSG Titans Security Group