תחקיר pCon 1365 | www.pCon.co.il | 23 נובמבר 2017

מניעת הונאות ומעילות

מסר אישי

מרכזיותן של מערכות המחשוב בעולם העסקים המודרני, הופכת אותן למטרה לניצול לרעה, כולל הונאות שונות. מסוכן במיוחד האיום הפנים ארגוני של מעילות עובדים, מהיותם בעלי גישה למידע רב ונהנים מאמון המערכת. במקביל, התרחבות עולם המחשוב לכיוונים חדשים, מציגה בפני פושעים מגוון הזדמנויות חדשות. לדוגמא - עסקאות אשראי, שבשנים האחרונות מתבצעות יותר ויותר מרחוק, ללא הצגת כרטיס אשראי. התוקפים מנצלים זאת וארגונים ניזוקים, נשארים מאחור ובאפילה, כאשר לפעמים הונאה פעילה, מסבה להם נזק מתמשך.

כיצד המנמ"ר יכול לסייע בתחום זה? מהם הכלים שבאמצעותם מנטרים, בולמים, מתריעים ומנתחים הונאות? אילו דוגמאות ממחישות את האיומים? על כך ועוד, בתחקיר שלפניך.

תוכן התדרוך השבועי

מה מגלה התחקיר?

אלה שאלות מפתח קריטיות, עליהן עונה התחקיר:

1. באיזו תדירות מתרחשות המעילות בארגונים?
2. כמה המעילות עולות לארגונים בכסף?
3. בכמה זינק היקף ההונאות הפעילות ברשתות החברתיות?
4. כיצד מומלץ למנמ"ר לטפל בכך, לפי **עידו נאור**, חוקר בכיר בצוות החוקרים הבינלאומי של **קספרסקי**?
5. בכמה עשוי לצמצם את גובה ההפסד, השימוש בסקירות לאיתור מוקדי סיכון?
6. מה אומרים על איתור דפוסי התנהגות חריגים, **עופר אלקלעי וגיא מונרוב**, מחברת **אלקלעי מונרוב**?
7. כיצד בלוקצ'יין מתבטא בתחום זה?
8. האם משתלם לבנות מערכת מחשוב לטיפול בהונאות או לרכוש אחת?
9. מהן ההשלכות של התראות שווא?
10. האם מטבעות וירטואליים הם בעצם הונאה?

לתשומת לבך

תחקירי pCon מתמקדים בכל מה ששימושי וחשוב בעולם המחשוב. הם מציגים באופן בהיר, אמין ומתומצת, את הטכנולוגיות המבטיחות, האיומים המשמעותיים ותפיסות המחשוב החדשות, למי שזמנו קצר ויקר. בכל נושא ניתן מיקוד בתועלתו, מגבלותיו, משמעויות יישומו והשלכותיו.

- **כל הזכויות שמורות לקומרקטינג בע"מ** ©. אין לצלם או להפיץ את הגיליון ללא היתר ובכל צורה שהיא.
- אנו משתדלים להביא מידע אמין ומדויק אולם האחריות לתוצאות השימוש בו תחול על המשתמשים.
- שמות המוצרים והחברות המוזכרים ב-**pCon**, הם שמות שמורים של בעליהם.

ליצירת קשר

עורך ראשי..... **קובי שפיבק MBA, B.Sc**
עורך..... **עמית לוי**
תחקיר וכתיבה..... **עמית לוי**
צלם מערכת..... **עזרא וישניא**
טלפון..... **03-9667939**, פקס..... **03-9660310**
דואר..... **דרבלה 10 / ת.ד. 2340 ראשון לציון 75121**
דוא"ל..... sub@pcon.co.il

1365.21 - סיכום למנהלים

בלימת, ניטור וניתוח מקרי הונאה, הם באופן שוטף חלק מפעילות כלל ארגונית, שיטתית ואסטרטגית, של ניהול הסיכונים. המנמ"ר יכול וצריך להיות מעורב בכך, לפחות משתי סיבות מרכזיות. האחת - היות המחשוב אמצעי מרכזי לביצוע הונאות. השנייה - היותו אמצעי משמעותי אפילו יותר, בניטור שוטף, בלימת נזקי הונאות, התראה, איסוף מידע וניתוח. למעשה, המנמ"ר מעורב בכך בעקיפין, מאחר שהיבטים רבים של אבטחת מערכות המחשוב, מסייעים גם לטיפול בהונאות.

"מעילה" היא זווית מיוחדת של הנושא. זהו סוג הונאה, שכולל היבט של הפרת אמון מיוחד שניתן לעבריין. אמון כזה, מתבטא פעמים רבות בהרשאות גישה למערכות מחשוב רגישות. מעילה בולטת במיוחד, הייתה המעילה של **אתי אלון**, ב**בנק למסחר**. סוג מתוקשר של מעילות, הוא העברת אגורות או עיגול סכומים לטובת חשבון מעבר, שנמשך על ידי המועל.

המגמות העיקריות שרואים בנושא זה כיום, כוללות את רמת ההונאות שמשתפרת, גישה מתרחבת של עובדים למידע ארגוני רגיש, טכנולוגיות חדשות כמטרה להונאות, הפיכת הארגון מ"גן סגור" של טכנולוגיה ל"גן פתוח", השפעת ה-**AI** ולמידת המכונה וכן הסתמכות הולכת וגדלה על אוטומציה עם בקרה מוגבלת. עוד נזכיר את בלוקצ'יין, כאחד הפתרונות העתידיים לתחום.

הונאות באמצעות המחשוב, עשויות להתבטא בין השאר במשלוח מייל מטעה, הונאות פיננסיות לסוגיהן, פישינג וגניבת זהות, שיבוש מידע במערכות הארגון, **Fake news** והונאות ברשתות החברתיות.

אתגרים בולטים, בהתמודדות עם הונאות ומעילות מבוססות מחשוב, כוללים את מורכבות מערכות המחשוב, האיום הפנים ארגוני שמסוכן במיוחד, היבטי פרטיות ואבטחה, נכונות ההנהלה להשקיע בכך, איכות המידע שמנתחים וכן השלכות של ריבוי התרעות שווא.

לפי **PwC**, מחקרים וסקרים של **האיגוד העולמי לחקר מעילות והונאות** (**ACFE**) מראים כי ברוב הארגונים מתרחשת מעילה משמעותית, לפחות אחת לשנה. ריכוז נתונים נוספים בנושא זה, מחברת **EY**, ראה כאן - fraudsurveys.ey.com

<u>לסיכום - כדאי להשקיע את הזמן הנדרש, בכדי לוודא שמחלקת המחשוב תורמת את מיטבה, לטיפול הכלל ארגוני בנושא קריטי זה.</u>

1365.22 - מגמות שמשפיעות על הונאות

אלה המגמות העיקריות, שרואים בנושא זה כיום:

- **רמת ההונאות עולה** - הונאות מתחילות פעמים רבות, אחרי שהתוקפים אספו מידע על הארגון הספציפי, כולל בעזרת נוזקה שפועלת בשקט בארגון לאורך זמן. כך, הם יכולים לזייף בצורה משכנעת במיוחד, מיילים מגורמים ספציפיים בארגון או בין ספקיו עם מסמכים שנראים אותנטיים.
- **גישה מתרחבת למידע** - ישנה גישה מתרחבת של מספר הולך וגדל של עובדים למידע. כתוצאה מכך, יותר אנשים חשופים למידע ארגוני, שניתן לנצל לרעה.
- **כניסת טכנולוגיות חדשות** - הפושעים מתמקדים במיוחד בסביבות מחשוב חדשות שהופכות לפופולאריות, אם זה מכשירים (סמארטפונים למשל), אפליקציות (כמו **ווטסאפ**) או אתרים (כ**אמאזון**).
- **מורכבות** - המורכבות הגדלה של מערכות המחשוב מסבכת את השליטה והבקרה וגילוי הונאות הופך להיות מורכב יותר. במקביל, השתכללות האוטומציה עשויה לסייע בניטור והתרעה בזמן אמת.
- **הפיכת הארגון מ"גן סגור" ל"גן פתוח"** - השימוש העסקי בסמארטפונים, כולל פרטיים ובשירותי ענן, הופך את סביבת המחשוב של הארגון למגוונת מתמיד. בהתאם, גובר הסיכון להונאות באמצעות המחשוב. **Shadow IT** מחמיר זאת ו-**BYOD** מסייע במידת מה.
- **AI ולמידת מכונה** - סטארט אפים שונים, מציעים כיום פתרונות זיהוי ומניעת הונאות, שמבוססים על למידת מכונה (תחום משנה של אינטליגנציה מלאכותית). עוד נציין בהקשר זה, כי השימוש ב-**BI** בתחום גילוי ההונאות, וותיק ומתרחב.
- **אוטומציה** - הסתמכות הולכת וגדלה על אוטומציה עם בקרה מוגבלת. פעמים רבות, האוטומציה מקלה לבצע הונאות מתמשכות במאמץ קטן ובמקביל היא מקטינה את הסיכוי שיבקרו אותה.

1365.23 - במה זה מתבטא?

הונאות באמצעות המחשוב, עשויות להתבטא בין השאר ב:

- **מייל מטעה** - משלוח מייל מטעה, ברמה שהולכת ומשתכללת, הוא רק צעד אחד במהלכה של הונאה, אך מדובר בגישת תקיפה מרכזית מאוד, שרבים נופלים ברשתה.
- **הונאות פיננסיות** - במערכות המחשוב, נעשה חלק בולט מההונאות הפיננסיות לסוגיהן. הונאות אלה, עשויות להשתמש לרעה במגוון אובייקטים מבוססי מחשוב, בהם כרטיסי אשראי, סמארטפונים ואתרי מסחר אלקטרוני.
- **פישינג וגניבת זהות** - פישינג הוא הוצאת מידע במרמה ובפועל, מדובר לרוב בפרטי זיהוי של הקרבן. למרות שפישינג יכול לשמש למגוון מטרות, כמו איסוף כתובות אימייל לשם משלוח ספאם, הוא משמש במקרים רבים כבסיס לגניבת זהות והתחזות ולאחר מכן, לניצולן לרעה.
- **שינוי מידע** - שיבוש מידע במערכות הארגון, על ידי האקרים שחודרים למערכות, באופן שיוצר תיאור מצב שיקרי. המטרה יכולה להיות למשל, כיסוי על גניבה.
- **Fake news** - מידע שמוצג כחדשות לגיטימיות, אך הוא למעשה שיקרי או פרשנות מטעה במכוון של מידע אמיתי. יש הונאות, שמנסות לפתות אנשים לפתוח מיילים או ללחוץ על קישורים, בכך שמבטיחים להם ששם הם כביכול יימצאו מידע נוסף, על "חדשה" מזויפת כזו.
- **הונאות ברשתות החברתיות** - כבר ב-2013, הונאות ברשתות חברתיות היו תופעה בולטת (bit.ly/fraud-social). כיום, המצב חמור הרבה יותר ומחמיר. ב-2016 זוהו 250,000 הונאות פעילות ברשתות החברתיות וב-2017 המספר כבר זינק ל-437,165 (**ZeroFox**).

1365.31 - על מעילה וכלכלה

מעילות והונאות מתבטאות לרוב בנזקים כלכליים לארגונים. אם לא כהפסד מיידי, לכל הפחות כנזקים כספיים מתמשכים של פגיעה במוניטין (למשל, לקוחות וספקים שחוששים לעבוד עם הארגון ועובדים שחווים פגיעה במוראל). לפי **PwC**, מעילות עולות לארגונים כ-6% מהרווח הגולמי באופן מצטבר, בממוצע. השימוש בסקירות לאיתור מוקדי סיכון, עשוי לצמצם את גובה ההפסד, בכ-40% בשנה. עוד על גובה נזקי ההונאות, ראה אינפוגרפיקה של **the Association of Certified Fraud Examiners** - bit.ly/fraud-31

על הפגיעה במכירות כתוצאה מהונאות, מרחיבה הכתבה הבאה - bit.ly/fraud-32

כמו בעולם האבטחה בכלל, הנדסה חברתית היא ערוץ תקיפה ראשי, בין אם זה מייל מגורם חיצוני שמנסה להטעות עובד או עובד מושחת שמנסה להטעות את מחלקת הנהלת חשבונות. החדשות הטובות, הן שההגנה מהנדסה חברתית זולה יחסית ולכן ה-**ROI** שלה גבוה במיוחד. הגנה זו, מתבטאת בעיקר בשני אמצעים שיחסית פשוט, זול ומהיר ליישם, הן חד פעמית והן באופן מתמשך - הדרכה ותרגול.

מהיבט אחר, מערכות מחשוב שמעורבות בניהול כספים בארגונים, משחקות פעמים רבות תפקיד מרכזי בפעילויות הונאה ובמיוחד מעילה (של גורם פנים ארגוני). בין אם זה המצב או שדווקא מערכת מחשוב אחרת בארגון רגישה יותר, אסטרטגיית האבטחה של הארגון צריכה במילא להתחיל (ולהתעדכן באופן שוטף) מהגדרת הנכסים העיקריים שעליהם יש להגן. כך גם ההשקעה הכספית במניעת הונאות, תפיק את המיטב, במגבלות התקציב.

האם משתלם יותר לבנות לבד מערכת מחשוב לטיפול בנושא זה? לפי דו"ח חברת **Kount**, התשובה משתנה בהתאם לנסיבות. להרחבה, ראה - bit.ly/fraud-33

1365.32 - שיקולים בבחירת הכלים

ישנם סוגים רבים של מוצרים ושירותי עזר בתחום ההונאות. אלה השיקולים המומלצים, בבחירת כלי ניתוח ותחקור:

- **מוניטין המוצר** - מניעת הונאות הוא נושא קריטי עסקית ולכן, זהו אחד התחומים שבהם מוניטין המוצר משמעותי במיוחד. בנוסף, כמו בעולם ה-**BI** בכלל, יש כאן אלגוריתמיקה מתוחכמת ומאחר שהיא בחלקה מאחורי הקלעים, רוצים לדעת בביטחון סביר, שמקבלים מוצר איכותי.
- **הספק** - מה שמציע ספק המוצר, בין אם הוא היצרן או משווק מקומי, מהיבטים כהדרכה, תמיכה ועדכון המוצר. נזכיר, שטיפול בהונאות ומעילות עשוי לדרוש פניה לספק לסיוע ועליו להיות מסוגל להגיב במהירות ולהיות דיסקרטי ואמין.
- **נוחות שימוש** - נוחות השימוש, תעודד שימוש נרחב ותפיק מהמוצר את המיטב. זאת, הן מהיבט קלות השימוש בממשק המשתמש והן מהיבט האפשרויות שהכלי מספק, למשתמשים ברמות מיומנות שונות. עוד היבט - עד כמה מפורטים וברורים ההסברים שהתוכנה מציגה, להמלצותיה והתרעותיה?
- **יכולות טיפול במידע** - היקף היכולות מבחינת טיפול במידע. זאת, כולל כמויות המידע שבהן ניתן לטפל בזמן אמת וכן מקורות מידע ופורמטי קבצים, שבהם ניתן להשתמש. כמובן, באופן ספציפי, חשובה האינטגרציה למערכות הארגון וההתאמה למקורות המידע וסוגי המידע שלהם הארגון זקוק כעת.
- **יכולות ניתוח** - חשוב שהכלי יציע ניתוחים מובנים וגם אפשרויות להתאמה אישית עם כתיבת סקריפטים ולאוטומציה של בדיקות ביקורת שונות.

מעבר לנקודות אלה, רצוי מאוד שהכלי יציע גם **Profiler** (ניתוח משתמשים וגיבוש פרופילים שלהם באופן אוטומטי), יבצע גם מניעת הונאות (ולא רק זיהוי והתרעה) וישתמש בלמידת מכונה לשכלול פעולתו (מעבר לאופני פעולה שמוגדרים מראש).

דגש - האם המטבעות הוירטואליים הונאה?

ביטקוין הוא הונאה, לדעתו של מנכ"ל ג'יי פי מורגן, ג'יימי דיימון. ראה ב**דה מרקר** - bit.ly/fraud-coin1 לפי מנכ"ל בנק **קרדיט סוויס**, ביטקוין הוא "הגדרה מדויקת לבועה" (bit.ly/fraud-coin2). למעשה, עוד ב-2014 תיאר **וורן באפט** את מטבע הביטקוין כ"אחיזת עיניים" (**כלכליסט** - bit.ly/fraud-coin3). שמא תאמר, שהביטקוין נמצא במרכז הבמה בעולם "המטבעות הקריפטוגרפיים" ולכן סופג גם לא מעט ביקורת. אז מה לגבי מטבעות אחרים? ראיון ב**כלכליסט** עם מייסד מטבע שהפך במהירות לאחד מחמשת המובילים, מוסיף עוד כמה סימני שאלה - bit.ly/fraud-coin4

1365.33 - ספקים לאמצעי מניעה

זו היא שורת ספקים בולטים בתחום מניעת ההונאות:

- **אלקלעי מונרוב** - מציעה תוכנה לבקרה פנימית מתמשכת, שמנטרת תחומי פעילות שונים בארגון, דוגמת שכר, רכש או ספקים, ומציפה חריגים בזמן אמת. מבוסס על המוצר **ACL**, ש**אלקלעי מונרוב** מייצגים בארץ - almo.co.il
- **יבם** - מציעה כלים נגד הונאות של חברת **Trusteer** הישראלית שהיא רכשה (www.trusteer.com), את שרות הענן **Counter Fraud on Cloud** (bit.ly/fraud-ibm1) וייעוץ - bit.ly/fraud-ibm2
- **קספרסקי** - מציעה הגנות נגד התקפות מסוגים שונים, כולל הגנות לאימייל ולשרתים. לפי החברה, גם המודיעין החזק במיוחד שהיא מציעה משמעותי למניעת הונאות וכן העובדה שכל מוצריה פותחו פנימית ולא דרך רכישות - securelist.com
- **BioCatch** - פתרון מעניין לזיהוי והתרעה על משתמשים לא מורשים (אנושיים או לא). הרעיון הבסיסי, הוא לזהות דפוסי התנהגות שימוש במקלדת ועכבר. לכך, החברה מוסיפה "הפרעות" יזומות וזעירות, בכדי לאלץ תגובה לא מודעת, שמסייעת לניתוח - www.biocatch.com
- **EMC - RSA**, חטיבת האבטחה של **EMC** מציעה **Fraud and Risk Intelligence Suite**, שמגן בין השאר על פעילות ב**אינטרנט** ובהתקנים ניידים, בזמן אמת - bit.ly/fraud-rsa
- **IDEA** - תוכנה לבקרה וביקורת פנים. מאפשרת לבצע ניתוחים בנקודות זמן לפי דרישה וכן להפעיל תהליכי ניטור שוטף, במטרה לבחון את יעילות ואפקטיביות הבקרות הפנימיות, בהתאמה לדרישות הרגולציה - www.iacs.co.il
- **IsItYou** - חברה ישראלית, שמציעה הגנה מהונאות שמתבצעות באמצעות הטעיית מערכות זיהוי ביומטרי - www.isityou.biz
- **NICE** - מגוון פתרונות נגד הונאה לארגונים (bit.ly/fraud-nice), כולל הגנת הונאות על קונטקט סנטרים (bit.ly/fraud-nice1) ובמגזר הכספי - www.niceactimize.com
- **Paygilant** - מוצר להגנה מהונאות ברכישה דרך ארנקים אלקטרוניים, שמתבצעות מסמארטפונים גנובים - www.paygilant.com

עוד נזכיר, את **אינטל** עם **Saffron Anti-Money Laundering Advisor** (bit.ly/fraud-intel), **ארגוסקופ** (www.argoscope.com), **ביטרייט** (הגנה למשתמשי ביטקוין מול מקרי הונאה - www.bitrated.com), **Riskified** (www.riskified.com) שמסייע בתחום המסחר האלקטרוני ומוצרי **SAS** שבייצוג **מיה מחשבים** (bit.ly/fraud-sas).

1365.41 - מומחים מייעצים מהשטח

כך שמענו, משלושה מומחים בולטים למניעת הונאות:

עידו נאור, חוקר בכיר בצוות החוקרים הבינלאומי של **קספרסקי**, אומר כי אנו נתקלים כיום בהונאות שדומות מאוד להונאות שראינו בעשר השנים האחרונות, בעיקר ניצול קרבן בעל מודעות נמוכה לנושא. התוקפים מתמקדים בשירותים שהקרבן משתמש בהם בתכיפות וכיום מדובר למשל ב**ווטסאפ** או **פייסבוק**. ההונאות בכלל, משתנות בהתאם לשינויים אצל המשתמשים. התוקפים גם לומדים טוב יותר ויותר את אופי הקורבנות ו"תופרים" הונאה, לטובת תקיפת אותו משתמש. זה יכול להתחיל מהתחזות לאדם או לשירות. למשל, איש כספים בחברה שמקבל מייל מזויף, כביכול מהמנכ"ל, עם בקשה להעביר כספים. אלה דברים שלא דורשים יכולות טכנולוגיות, אלא יכולות מודיעיניות. יש גם קבוצות האקרים עם מימון גבוה, שפורצים לבנקים, מתמקמים על שרת העברות הכספים (המחובר לרשת העברת הכספים **Swift**) ושולחים לבנק המרכזי בקשות להעביר כסף. התוקפים גם משתמשים בבלוקצ'יין, במסגרת ביטקוין כאמצעי תשלום. מצד שני, יש שמשתמשים בבלוקצ'יין להגנה, עבור אימות. מבחינת מה שניתן לעשות בכדי להתגונן, יש כיום מוצרי אבטחה רבים מאוד, כולל שוק מתרחב של סטארט אפים בתחום מניעת ההונאות. עם זאת, בשנים האחרונות גם הופיעו סביבם המון "מילים גדולות" וארגונים רבים נכנסים לעולם זה, כאשר אין להם מושג מה הם עושים. לאחר הקניה, הם מבינים שאין להם דרך לנהל זאת. מומלץ לטפל קודם בדברים הפשוטים. לנסות להבין מה סוג הרשת? על מה אני מגן? היכן נמצאים הנכסים? כיצד מונעים מהעובדים עצמם להתקיף את הארגון? ואז, אם צריך לייצר הגנה מיוחדת חייבים יועץ אבטחה מוסמך עם רקורד, שאיתו ניגש לרכוש את המוצרים. הצעד שיצמצם את ההונאות למינימום, הוא לחנך את העובדים בצורה טובה - תקשורת בין העובדים, ההנהלה והמחשוב. אגב, עובדים אוהבים להיכנס כשותפים לזיהוי במקרי תקיפה כאלה. המנמ"רים לפעמים סומכים יותר מדי על מי שמספק להם את ציוד הרשת או מי שמנהל את ה-**IT**. השורה התחתונה, היא להתעניין. מנכ"לים צריכים לתת את הסמכות למנהל המחשוב וגם הוא צריך לדרוש זאת. המנמ"ר גם יכול להוכיח את הצורך במהירות, בכך שהוא יעביר מאמרים בנושא זה או ייזום תהליכי לימוד.

עופר אלקלעי וגיא מונרוב, מחברת **אלקלעי מונרוב** (☎ 03-6125612) מציינים כי בעזרת המחשוב, ניתן לאתר דפוסי התנהגות חריגים. ממפים את הארגון מבחינת תהליכי עבודה, מזהים דפוסי פעולה חוזרים ומחפשים אינדיקציות, היכן עשויה להיות הונאה? אם מזהים אנומליה, ניתן לשאול "למה?". למשל, ספק שהיה "רדום" במשך שנים ופתאום מתחיל להיות פעיל, ספק שמשנה פרטי חשבון בנק פעמים רבות, פקודות יומן בשעות חריגות או פקודות יומן לא סבירות, כגון ספק מול ספק. הרעיון, הוא להשתמש בכלים סטטיסטיים, לשם הבנת המידע הקיים וקבלת תובנות על אנומליות. לשם העולם הולך בתחומי פעילות רבים. זהו סוג של **BI** ולמידת מכונה, על המערכות התפעוליות בארגון. מבחינת הונאות בנוסח "העוקץ הניגרי", בעבר היו נשלחים אלפי מכתבי הונאה בדואר רגיל, בעלויות גבוהות מאוד. כיום, בעזרת זמינות ה**אינטרנט** והיכולת להשיג מאגרי מידע עצומים, הפושעים יכולים לשלוח כמויות אימיילים אדירות, בעלות זניחה. עם זאת, "הסיפורים" שאותם רמאים מספרים, נשארו אותם סיפורים. הרבה יותר מדאיג מכך, זו תופעת הנוכלים שעוקצים ארגונים, בהתחזות לספק שלהם. זאת, כאשר הם משתמשים בכתובת דואר אלקטרוני, אשר כמעט זהה לזו של הספק האמיתי. בעזרתה, הם למשל מבקשים לשנות פרטי חשבון בנק של הספק. זו היא תופעה רחבה, שיש נוכלים שמתמחים בה. יש גם דוגמאות רבות של הונאות על ידי עובדים מהארגון, כמו נציגי שירות, שניצלו את המידע שהיה ברשותם על הלקוחות. המלצה מעשית חשובה, היא לבצע בדיקה לגילוי הונאות, פעם בחודש עד פעם ברבעון. כמו כן, אם משתמשים במחשוב ענן, חשוב לבדוק את היבטי האבטחה של הספק.

1365.42 - טיפים למניעה

טיפים אלה, יסייעו לקדם מניעת הונאות באמצעות המחשוב:

- **הגנה על הלקוח** - לעתים, הונאות פוגעות גם בלקוחות הארגון. למשל, במקרה של נוכל שפונה אליהם, תוך התחזות לנציג הארגון או פונה לארגון, עם פרטי זהות גנובים של הלקוח. מודעות, יכולת תגובה מהירה, תיעוד וחקירה, עשויים לצמצם נזקים של מקרים כאלה, ללקוח ולארגון (כולל נזקי תדמית).
- **פספס, פספס, ששש...** - כדאי להרגיל עובדים, לזהות סימנים חשודים במיוחד במיילים. למשל, זירוז לפעולה מהירה ובקשה לשמור על חשאיות. נאמר, מייל מהמנכ"ל כביכול להנהלת החשבונות, לסייע בפרויקט "דחוף ורגיש", ש"חשוב שלא לדבר עליו עם אף אחד!". הפתרון, הוא כמובן לא להגיב למייל ולדבר על כך בהקדם עם המנכ"ל.
- **רכישת דומיינים דומים** - בכדי לצמצם משמעותית את הסיכוי להקמת אתר שמתחזה לאתר הארגון, ניתן לרכוש דומיינים עם שמות דומים לשם אתר הארגון ובכך למנוע מפושעים לרכוש אותם.
- **שני צדדים למטבע** - כאשר מתרגלים את העובדים להיזהר מהונאות, אם אחד מהם מעורב במעילה נגד הארגון, הרי שבתהליך זה גם מתרגלים אותו, להתחמק מגילוי. לכן, מעבר להכרחי, מוטב לערב כמה שפחות אנשים במאמצי הארגון למניעת מעילות ומשמעותי במיוחד, סיוע מגוף חיצוני שמתמחה בכך.
- **למנף Low Tech** - קל להיעזר במערכות מחשוב לשם הטעיה והדרכים הממוחשבות להתמודד עם עובדה זו, פגיעות בעצמן והן אינן פשוטות או זולות. לכן, כדאי תמיד לזכור ולקחת בחשבון פתרונות פיזיים, פשוטים ואמינים יותר. למשל, להרים טלפון או להיפגש פיזית, בכדי לוודא שבקשת העברת כספים גדולה, אכן נשלחה אליך ממנהל **X**. כמובן, ההנהלה חייבת לתמוך רשמית בתהליכי אימות כאלה, אחרת זה לא יבוצע.

1365.43 - נקודות להיערכות

כך מומלץ לקדם שיטתית, מניעת הונאות ומעילות:

1. **להשקיע את הזמן** - מאחר שלא מדובר בנושא שמניב תועלות עסקיות מיידיות, יש תמיד דברים דחופים יותר לעשות. לכן, יש להתחיל מהגדרת הנושא כחשוב, להקצות לו זמן מספיק ופשוט להתחיל לקדם זאת, גם אם הדרגתית.
2. **תיאום אסטרטגי** - הטיפול בהונאות ומעילות איננו בהובלת המנמ"ר. אגף המחשוב משתלב בנושא, כחלק מהטיפול הכלל ארגוני בכך, שבעצמו כלול ב-**GRC** (או **Governance, risk management, and compliance**). לכן, חיוני לקדם שיתוף פעולה עם ההנהלה בנושא זה ולחשוב ולתאם ביחד, האם וכיצד, אגף המחשוב יכול לסייע ולשפר.
3. **אמינות באגף המחשוב** - לעובדי אגף המחשוב, עשויים להיות גישה והרשאות רחבות, למערכות מידע רגישות של הארגון. לכן, כדאי לבצע בדיקת רקע על מועמדים לעבודה, החל מחיפוש פשוט ב**אינטרנט** (שמעלה חלקית גם פסקי דין אגב) ועד בדיקת רקע רחבה יותר במידת הצורך.
4. **בקרת גישה** - נושא בסיסי שחשוב לקדם בכל מקרה, באופן שוטף, הוא בקרת גישה חזקה למערכות המחשוב. זה יכול להיות באמצעות ביומטריה, סיסמאות חד פעמיות או ריבוי אמצעי זיהוי.
5. **חסימת דואר חשוד** - ניתן להתריע או לחסום, כאשר מייל מגיע מכתובת שאיננה ב"רשימה לבנה" של כתובת מורשות. ניתן גם לחסום או להתריע אוטומטית, כאשר מגיע מייל מכתובת שמתחזה לכתובת לגיטימית של הארגון, ספקיו ולקוחותיו העיקריים. הואריאציות שלא יעוררו חשד, לרוב מצומצמות בהיקפן. למשל **our_company@** במקום **our-company@**.
6. **הדרכה** - חיוני להדריך עובדים באופן שוטף, כיצד לזהות אינדיקאטורים להונאות ומעילות ומה לעשות במקרים אלה. אגף המחשוב עשוי להשתלב בכך, במיוחד בכל הנוגע להדרכה לגבי היבטי המחשוב.
7. **תרגול** - תרגול העובדים והמנהלים בתגובה נכונה לניסיונות הונאה ומעילה, יכול להתבצע במסגרת הטיפול השוטף של אגף המחשוב בתרגולם, לגבי התגוננות באבטחת המחשוב בכלל. זאת, כולל הסתייעות בשירותי בדיקות חדירה.

1365.51 - כיצד המחשוב מסייע?

אלה הם כמה היבטים, של שימוש במחשוב לשם הגנה מהונאות:

- **עבודה לפי תקנים ומתודולוגיות** - תקן **סרבנס אוקסלי** מגדיר כמה תהליכי עבודה מהותיים לדיווח כספי, בהם אבטחה, הרשאות ותפעול **IT** (תפעול שגוי, עשוי לשבש נתונים). הוא מתייחס גם לניהול שינויים ופיתוח מערכות מידע. אם מפתחים דו"ח פנימי שאמור לתאר מצב לקוחות ולפיו מדווחים בדו"חות הכספיים, שגיאה בדו"ח הפנימי, תתבטא גם בחיצוני. לפי **עופר אלקלעי וגיא מונרוב**, מ**אלקלעי מונרוב**.
- **בקרת גישה מרחוק למחשוב** - בקרת גישה למערכות מחשב, עם הקצאת וניהול הרשאות. ברמה מתקדמת, בקרת הגישה תתאים את עצמה באופן מתמשך, לעובד ולמצב שבו הוא נמצא. ראה באתר **CIO** - bit.ly/fraud-cont
- **בקרת גישה פיזית למחשוב** - בקרת גישה פיזית להתקני מחשוב של הארגון, שבהם נמצאים נכסים רגישים, שעשויים לשמש להונאה או למעילה.
- **בקרת גישה פיזית בסיוע מחשוב** - שימוש בזיהוי ביומטרי או בכרטיסי זיהוי, לבקרת גישה לנכסים פיזיים רגישים של הארגון.
- **ניתוח מידע** - ניתוח מידע ופעילויות במערכות המחשוב ובתקשורת, לשם זיהוי דפוסי מידע חשודים. כלי תחקור נתונים מקצועיים של מומחי ביקורת, מאפשרים לנתח מידע נרחב במהירות, במקום להסתמך רק על בדיקה ידנית של דגימות (שעשויה להיות איטית ושגויה).

עוד נזכיר, שמומחים חיצוניים עשויים להיות מוזמנים לביצוע ביקורת חקירתית בארגון. ביקורת כזו, בודקת במידה רבה את מערכות המחשוב, לרבות לסימני הונאה.

1365.52 - סיפורים מהחיים

זהו אוסף דוגמאות להונאות, שבהן היה מעורב מחשוב:

- **כרטיסים בחינם** - הונאה שרצה בימים אלו ב**ווטסאפ**, מציעה שני כרטיסי טיסה חינם בחברת **בריטיש איירווייז**. מובן שלא ללחוץ על הקישור ולהיזהר.
- **איתך בכל מקום** - הרמאים נמצאים, בכל מקום שבו משתמשי המחשב נמצאים והם "מתקדמים עם הזמן". לדוגמא, הונאת **ווטסאפ**, בה "חבר" ממליץ לך על שרות **WiFi** חינמי - bit.ly/fraud-up
- **טוב שיש מפתח "מאסטר"** - בארגונים רבים משתמשים בשירותים שונים של **גוגל** ובכתובות מייל ב**ג'ימייל**. מיילים שהתקבלו לחשבונות **ג'ימייל**, כביכול מאנשי קשר של הנמענים, ניסו להוציא מהם את פרטי הסיסמא הראשית לחשבונות אלה. היכן שהם הצליחו, הם קיבלו בכך גישה, ללא ידיעת הקורבן, לכל שירותי **גוגל** שאליהם הוא רשום - bit.ly/fraud-goo
- **פרשת גיא וייסמן** - המשנה לשעבר של בית ההשקעות בחברת **הראל**, הודה בשנת 2010 בגניבת 98 מיליון ש"ח (bit.ly/v-harel). לפי **עופר אלקלעי וגיא מונרוב**, מחברת **אלקלעי מונרוב, לווייסמן** היו הרשאות גורפות לכמעט כלל הפעילות וכך הוא יכל גם לטשטש עקבות.
- **לחשוב בגדול** - נאמר שאתם מחלקת הנהלת חשבונות של חברה קטנה עם תקציב אבטחה מזערי, שקוראים לה **גוגל** או **פייסבוק**. עכשיו נאמר שנוכל מציג עצמו כנציג יצרנית חומרה **מטייוואן** ומסביר שאתם חייבים ל"חברה" שלו סכום סמלי עבור שירותים ומוצרים שהוא סיפק (נאמר, 100 מיליון דולר). אין סיכוי שזה יצליח? כנסו, כנסו.. - bit.ly/fraud-goog-face

עוד דוגמאות מהשטח, ראה באתר **Fraud magazine** (bit.ly/fraud-case) וכן בעמודים 13 ו-14 בקובץ ה-**Pdf** הבא מחברת **PwC** - bit.ly/fraud-example

1365.53 - האתגרים בהתמודדות

אלה כמה אתגרים בולטים, בהתמודדות עם הונאות ומעילות מבוססות מחשוב:

- **מורכבות** - מורכבות מערכות המחשוב, מקלה להסתיר "מחט בערימת שחת". מהיבט אחר, גם מערכות מניעת וניתוח ההונאות, הן מורכבות יחסית.
- **האיום הפנימי** - הונאות מעובדים פנימיים נפוצות במיוחד, מסיבות רבות, בהן גישה למערכות פנימיות ומידע פנימי וכן היכרות (חלקית לפחות) עם אמצעי ונהלי האבטחה שעשויים להפריע למעילה.
- **פרטיות ואבטחה** - חקירת הונאות ומעילות יכולה להיעזר במידע רב על אנשים, אך לא כל מידע כזה ניתן להשיג באופן חוקי (היבט שמשתנה ממדינה למדינה). עשויים להיות גם חוקים מחייבים, לגבי שמירתו ואופן ההגנה עליו.
- **נכונות להשקיע** - מנהלים מבינים היטב, שמדובר בנושא קריטי. עם זאת, ההשקעה השוטפת שנדרשת עבורו עשויה להיות מוזנחת, בגלל דברים שנתפסים כדחופים יותר. כמו לגבי אבטחה, נושא שאמור להניב תועלת עסקית בטווח הקרוב עשוי לזכות ליותר משאבים ותשומת לב מנושא כהונאה, שכל עוד לא גילינו כזו, מהווה (כביכול) רק מקור להוצאות.
- **איכות מידע** - מערכות לגילוי, בלימת וניתוח הונאות ומעילות, מסתמכות במידה מכרעת על ניתוח מידע רב. מידע זה עלול להיות באיכות נמוכה - חלקי, מיושן או לא סטנדרטי (כתאריכים, שחלקם בפורמט כזה וחלקם בפורמט אחר). בהתאם לכך, תוצאות עיבוד המידע עלולות להיפגם.
- **False positives** - כמו בעולם האבטחה בכלל, ניתן להניח שגם במניעת הונאות, עדיפה מערכת מחמירה, גם במחיר של ריבוי התרעות שווא. מצד שני, התראות שווא בנושא הונאות ומעילות, עשויות להפריע לפעילות השוטפת ואף להביא להחלטה על צמצום העבודה מול גורמים מסוימים (לקוחות, ספקים או שווקים), אולי שלא בצדק.

1365.54 - קישורים שיסייעו במניעה

אלה הם מספר קישורים מעניינים בנושא הונאות ומחשוב:

- **ACFE** - the Association of Certified Fraud Examiners מציע אתר ובו מאמרים רבים בנושא זה ומקורות מידע נוספים - www.acfe.com
- **הונאות בתשלומים** - על תופעת ה-**Payment Fraud** ואופני ההתמודדות איתה, בסרטון הבא של חברת **יבמ** - bit.ly/fraud-pay
- **החוליה החלשה** - **גרטנר** מזהירה כי **Contact centers** הם חוליה חלשה בארגונים מבחינת הונאות. עוד על כך ועל הדרכים האפשריות לשיפור המצב, באתר **ZDNet** - bit.ly/fraud-contact
- **מסחר בטוח** - 7 עצות, להגנת אתר מסחר אלקטרוני מהונאות וסיכונים נוספים, מביא אתר **CIO**, במאמר הבא - bit.ly/fraud-site
- **בלוקצ'יין מאבטח** - על הרעיון של שימוש בבלוקצ'יין לשם צמצום הונאות בניהול חשבונות בארגונים, מרחיב המאמר הבא באתר **CPA Journal** - bit.ly/fraud-blo
- **החיקוי והמקור** - **Lyrebird** היא תוכנה שמחקה קולות אנשים, אשר מפתח סטרטאפ קנדי. בינתיים, היא לא מי יודע מה משכנעת, אבל הפוטנציאל השלילי, כולל להונאות, ברור. הדגמה ודיון על כך, בסרטון הבא - bit.ly/fraud-voice
- **Benford's Law** - אם מתמטיקה גורמת לך לפהק, נסה את הסרטון הבא (טריק מתמטי מעניין, לזיהוי הונאות)! - bit.ly/2zDqZCv

איך לחבר את הטכנולוגיה לחיים?

קוראים יקרים

מתוך כוונה להפוך את קריאת תחקירי pCon, להזדמנות לקבל הבנות שמקדמות אתכם, אני מזמין אתכם לאחר קריאת התחקיר, להקדיש עוד רגע קצר כדי להבין את ההשלכות המעשיות עבורכם, של יישום הטכנולוגיה והיבטיה השונים. לשם כך, ענו לעצמכם על השאלות למטה (רצוי מאד בכתב), כך שתוכלו לראות ולהבין באופן חד וברור, מתי וכיצד הטכנולוגיה תוכל להתחבר למציאות המעשית והמקצועית שלכם, לסייע לכם ולקדם אתכם. כך גם חווית העדכון המקצועי, תהפוך ליותר מלהיבה, מעוררת עניין ומשמעותית.

אשמח לקבל משוב והתייחסויות לתוספת זאת, למייל שלי - koby@pcon.co.il לטל' 054-4301728 או לדף הפייסבוק שלנו - bit.ly/pcon_facebook

בברכה לבבית,

קובי שפיבק - העורך הראשי של pCon

השאלות להבנה

- **ההבנה החדשה** - מהי ההבנה העיקרית החדשה, שקיבלתם מהתחקיר?

_____

- **הפעילות המעשית** - איזה פעילות מעשית (שינוי), כדאי לעשות לאור ההבנה החדשה? למה ובאיזו מידה, הפעילות הזאת נראית לכם חשובה (0 - 100)?

_____

- **המדד להצלחה** - מה צריך לקרות או מה יהיה המדד החד משמעי, לפיו תשתכנעו שהצלחתם לקדם נושא שחשוב לכם? מתי תבחנו זאת?

_____

- **עזרה זמינה** - מי (עובדים, יועצים, ספקים) או מה (התייעצות, קריאת מידע נוסף) יסייעו לכם, לקדם את הפעילות שנראית לכם?

_____

- **הצעד המידי הראשון** - מהו הצעד הראשון שכדאי לנקוט בו עכשיו, כדי לחבר את הטכנולוגיה לחיים, וליצור אצלכם מציאות חדשה שמקדמת אתכם?

_____

התרומה העסקית לארגון, בעקבות צמצום הונאות ומעילות בתחום המחשוב

המטרה - מזכר זה מצביע על תועלות והשלכות אפשריות, מצמצום הונאות ומעילות, בתחום המחשוב.

התרומה האפשרית לארגון - צמצום הונאות ומעילות בתחום המחשוב, עשוי לתרום להשגת יעדים עסקיים, כמו צמצום סיכונים, צמצום הפסדים כספיים, מניעת פגיעה במוניטין הארגון, שיפור הרציפות העסקית, חיזוק אבטחת המחשוב בכלל ושיפור התאימות לתקנות בפרט.

רקע קצר - מרכזיותן של מערכות המחשוב בעולם העסקים המודרני, הופכת אותן למטרה לניצול לרעה, כולל לסוגים שונים של הונאות. מסוכן במיוחד האיום הפנים ארגוני של מעילות עובדים, מהיותם בעלי גישה למידע רב ונהנים מאמון המערכת. במקביל, התרחבות עולם המחשוב לכיוונים חדשים, מציגה בפני הפושעים מגוון הזדמנויות חדשות. לדוגמא - עסקאות אשראי, שבשנים האחרונות מתבצעות יותר ויותר מרחוק, ללא הצגת כרטיס אשראי. התוקפים מנצלים זאת וארגונים לעתים נשארים מאחור ובאפילה, בעוד הונאה פעילה מסבה להם לפעמים נזק מתמשך.

במה זה מתבטא? - הונאות באמצעות המחשוב, עשויות להתבטא בין השאר במשלוח מייל מטעה, הונאות פיננסיות לסוגיהן, פישינג וגניבת זהות, שיבוש מידע במערכות הארגון, Fake news והונאות ברשתות החברתיות.

דגשים לתשומת לב - האתגרים הבולטים, בהתמודדות עם הונאות ומעילות מבוססות מחשוב, כוללים את מורכבות מערכות המחשוב, האיום הפנים ארגוני שמסוכן במיוחד, היבטי פרטיות ואבטחה, נכונות מעטה מדי להשקיע בכך, איכות המידע שמנתחים וכן השלכות של ריבוי התרעות שווא.

היבטים כלכליים - מעילות והונאות מתבטאות לרוב בנזקים לארגונים, שלפחות חלקם כספיים. אם לא כהפסד מיידי, לכל הפחות כנזקים כספיים מתמשכים של פגיעה במוניטין (למשל, לקוחות וספקים שחוששים לעבוד עם הארגון ועובדים שחווים פגיעה במוראל). לפי PwC, מעילות עולות לארגונים כ-6% מהרווח הגולמי באופן מצטבר, בממוצע. מאידך, השימוש בסקירות לאיתור מוקדי סיכון, עשוי לצמצם את גובה ההפסד, בכ-40% בשנה.

הצעה להרחבה - במידה והנושא נראה לכם מעניין, אשמח להכין עליו, נייר עמדה מפורט.

דגשים למכיני המזכר:

- *מזכר זה נועד לשתף חברי הנהלה נבחרים, שיהיו מעוניינים לראות ולהבין את התועלות וההשלכות לארגון, מיישום הטכנולוגיות והתפיסות החדשניות, שמשנות את העולם העסקי.*
- *כדי לעורר עניין, המזכר מציג את הטכנולוגיה מבחינת תרומה לערכים עיקריים שחשובים לחברי ההנהלה: צמיחה מואצת, קיצור זמנים, גמישות, הפחתת הוצאות וסיכונים וכדומה.*
- *ניתן להציג את הנושא בשיחה קצרה **או לשלב במייל בשיטת העתק והדבק**, תוך התאמת הדברים לנושאים העסקיים שעל הפרק או השמטת מסרים שאינם רלוונטיים.*
- *כדאי לשים לב למתכונת המצומצמת של המזכר, כ-300 מילים.*
- *המזכר מתבסס על תחקיר 1365 "מניעת הונאות ומעילות" (כך שאין צורך לחפש מידע או להשקיע זמן רב בהכנה) וניתן להתבסס עליו, בהכנת נייר עמדה להנהלה.*