המכון לחקר המתודולוגיה של המודיעין

המרכז למורשת המודיעין

16 באוגוסט 2020

כנס בנושא התקפות סייבר ומודיעין בתקופת הקורונה

המכון לחקר המתודולוגיה של המודיעין קיים ב-13 באוגוסט 2020 כנס מקוון בנושא התקפות סייבר ומודיעין בתקופת הקורונה. מטרות הכנס היו לתאר את ההיערכות המודיעינית מול האתגר מזוויות שונות (המגזר הציבורי, המגזר הפרטי, מכוני המחקר והמגזר השלישי), וללמוד מכך על ההתמודדות המודיעינית בתחום הסייבר גם בהקשרים אחרים.

את הכנס הנחה סגן ראש המכון, דודי סימן-טוב, והשתתפו בו סא"ל (מיל.) דניאל ראקוב, לשעבר מאמ"ן וכיום עמית מחקר במכון למחקרי ביטחון לאומי; אל"מ (מיל.) שי שבתאי, לשעבר מאמ"ן וכיום האסטרטג של חברת Konfidas; לביא שטוקהמר, מנהל ה-CERT במערך הסייבר; סנז ישר, לשעבר מאמ"ן וכיום אנליסטית סייבר ראשית ומרכזת תחום המחקר ומודיעין סייבר ב-FireEye ישראל; ואוהד זיידנברג, מייסד CTI League, וחוקר מודיעין סייבר בכיר ב-ClearSky Cyber Security.

להלן התובנות המרכזיות שעלו בכנס:

<u>מציאות חדשה – סיכונים והזדמנויות</u>

תקופת הקורונה מזמנת סיכונים רבים בתחום הסייבר, בדגש על מערכות הבריאות, כפי שכבר הומחש לאחרונה במספר אירועים. חוסר הוודאות והשינויים באורח החיים מגבירים סיכונים אלה. חלק משינויים אלה עתידים להישאר גם בחלוף הקורונה. עם זאת, נראה כי היא מביאה עמה גם אפשרות לגשר על מגבלות רעיוניות לאור אינטרס רחב משותף. <u>בכל מקרה מתחייבת היערכות מודיעינית מקפת להתגוננות מול מתקפות אלה.</u>

<u>הצורך להבין את ההיגיון האסטרטגי של התוקף</u>

פעולות התקפיות בסייבר של גורמים עוינים עלולות להיות חסרות פשר אלמלא לוקחים בחשבון את ההגיונות האסטרטגיים של התוקף. חשוב לעלות מ"קומת הביטים" לרמת התקיפה, אבל חשוב גם לרדת מההגיונות האסטרטגיים לרמת התקיפה (כלומר גם מלמטה למעלה וגם להפך).

<u>פרו-אקטיביות כחלק מההגנה בסייבר</u>

בנוגע להגנה בסייבר חשוב לשמור על אקטיביות (לחפש פרצות למשל) ולסכל את התקיפה בעודה מתרחשת כדי לגרום לתוקף לשאת באחריות לה. כדי לאפשר זאת יש להשקיע תשומות במניעה פרו-אקטיבית, קרי איתור יזום מתמשך של חולשות בהגנה.

<u>צורך בשת"פ ותיאום בין מגזרים שונים</u>

שיתוף פעולה בין המגזרים השונים ובין הגופים השונים הוא חיוני. אזור שלא מכוסה על ידי גוף אחד, יכול להיות מכוסה על ידי גוף אחר, הנהנה מיתרון היחסי. בנוסף, במקומות מסוימים כיסוי של יותר מגורם אחד מוביל לשיפור ולייעול עבודתם של הגורמים השונים.

סיכום את הכנס

ליאב סלע - עוזר מחקר במכון לחקר המתודולוגיה של המודיעין

<u>פירוט הכנס</u>

ראש המכון, תא"ל (מיל.) יוסי קופרוסר

המכון לחקר המתודולוגיה של המודיעין נידרש להפנות זרקור לסייבר בהיותו תחום מודיעיני מרכזי. קיימות התקפות סייבר כל הזמן, אך תקופת הקורונה מדגישה את הסיכון של תקיפות סייבר, בעיקר סביב נושאי בריאות, כשישראל בין השאר היא יעד לגניבת מידע רגיש למשל בנושא החיסון. ננסה להבין איך המודיעין מנסה להתמודד עם סוגיה זו, בדגש על הפן ההגנתי.

סא"ל (מיל.) דניאל ראקוב – לשעבר מאמ"ן, כיום מהמכון למחקרי ביטחון לאומי

רוסיה לא רואה את הסייבר כמרחב שעומד בפני עצמו, אלא כחלק ממרחב המידע, וזה אחד המישורים הטכנולוגיים שבהם רוסיה מנהלת את מלחמת המידע כדי לקדם את יעדיה. לכך יש מספר דוגמאות בתקופת הקורונה:

א. ההצהרה על החיסון- ניסיון למצב עצמה כמנצחת במערכה על מציאת החיסון. יש הרבה ביקורת בעולם בנוגע לרישום החיסון הזה, שכנראה לא עומד באמות המידה הסטנדרטיות. לרוסיה חשוב מאוד להציג את עצמה כמתקדמת טכנולוגית, דווקא משום שהיא נתפסת כמפגרת טכנולוגית כלפי פנים וכלפי חוץ. בתוך כך, יצאה הודעה משותפת של סוכנויות ההגנה בסייבר של ארה"ב, קנדה ובריטניה, שרוסיה מבצעת תקיפות סייבר על מרכזי פיתוח בהקשרי הקורונה. יום למחרת ההודעה הזו, פורסם הסכם במסגרתו חברה רוסית תקבל את הידע על חיסון אחר (של חברה בינ"ל אסטרה-זניקה ושל אוניברסיטת אוקספורד), כך שלכאורה גניבת מידע היא מיותרת, ולכן ההודעה המשותפת לא רלוונטית. כנראה שלרוסים עדיין חשוב להשיג את כל פרטי המידע על מנת להיות ראשונים, בהקשר התודעתי. כמו כן, הטענה היא שמנסים להשיג מידע על פערים בחיסונים של אחרים, על מנת להחליש את מהימנותם בהמשך כשתהיה תחרות. כנראה שרק גנבו מידע על תקלות ולא שיבשו אקטיבית.

ב. תקיפות קיברנטיות בצ'כיה- בזמן הקורונה ארעה תקיפה נגד שורה של מוסדות לרבות בתי חולים. הרוסים הם החשוד המיידי אך לא הוכח שהם עומדים מאחורי התקיפה. היחסים של צ'כיה ורוסיה מעורערים בלאו הכי סביב כוונת ראש עירית פראג להסיר פסל שמציג נראטיב ניצחון רוסי במלחה"ע השנייה. זו לא הפעם הראשונה שהרוסים פועלים בתגובה לניסיון לשנות נראטיבים פרו רוסיים.

ג. ארה"ב - שורת תקיפות שמזוהה עם הGRU במהלך שנה וחצי, בתוך מוסדות ממשל פדרליים ובגופי אנרגיה, ככל הנראה על מנת לאותת שהרוסים יכולים לעשות כן, או במטרה להשיג מידע כלכלי על

אנרגיה, משום שאנרגיה היא עמוד תווך מרכזי בכלכלה הרוסית. גם בנושא הזה רוסיה פעלה כבר בעבר על מנת לפגוע בארה״ב בערוצי אנרגיה.

ד. העמקת שסעים בחברה האמריקנית- תקופת הקורונה העמיקה שסעים, למשל סביב היחס לאפרו-אמריקנים, ובעבר רוסיה פעלה על מנת להעמיק את השסע הזה ואחרים. רוסיה, דרך חברה פרטית רוסית, הקימה חוות טרולים ובוטים באפריקה, והפעילה קמפיין של הפצת פוסטים ליצירת שיח מקוטב בארה״ב.

מה לומדים מזה? כדי להבחין בתקיפות בסייבר ולהתגונן מולן חשוב להבין את הזווית של התוקף. מה ההיגיון בלתקוף בתי חולים? ובכן, בראי הרוסים, הנראטיבים ההיסטוריים הללו נחשבים אסטרטגיים והכרחיים, גם אם הדבר לא מובן מאליו. חשוב לעלות מהביטים לרמת התקיפה אבל חשוב גם לרדת מההגיונות האסטרטגיים לרמת התקיפה.

אל״מ (מיל.) שי שבתאי – האסטרטג של חברת Konfidas

היה אל״מ באמ״ן; בחמש השנים האחרונות הוא בחברת Konfidas שהיא חברת ייעוץ, ובשנה האחרונה אף עשה פרויקט גדול של הגנה בסייבר בחברת טבע; ומרצה בבר אילן. פרסם לאחרונה מאמר בנוגע לחיבור בין מאפייני הפעולה של המודיעין לבין מאפייני ההתגוננות מול התקפות סייבר-

https://medium.com/konfidas/when-cyber-and-intelligence-meet-analyzing-the-challenges-of-cyber-intelligence-in-incident-daba09216349

הרעיון במודל שמוצג במאמר הוא לחבר חמשת יסודות המודיעין - ידיעה, הבנה, הטמעה, השפעה והשתנות, יחד עם עקרונות ההתגוננות מול משבר סייבר - מוכנות, זיהוי, ניתוח, הכלה, הכרעה, התאוששות ותחקיר, ולשלב אותם בהקשר של מערכת הבריאות.

	שלב 0: מוכנות	שלב 1: זיהוי וניתוח	שלב 2: הכלה והכרעה	שלב 3: השבה ותחקיר
ידיעה	• מדינות • שיבוש וערעור אמון • מידע פרטי כ-IP	• זיהוי מהיר של המידע של הארגון שלי	• מודיעין לבלימת זליגת המידע	
הבנה				
הטמעה	• סוגי איומים <-> משמעות האיומים		• מודיעין למהלך לשחרור מידע (נוסף) מטעה (מקרון...)	• מיקוד מאמצי ההגנה בראיית למידת והתפתחות היריבים
השפעה				
השתנות	• סוגי האיומים • התאום עם המדינה			• איתור המידע כמאמץ מתמשך

לביא שטוקהמר – מנהל ה-CERT במערך הסייבר

ההתמודדות עם הקורונה גורמת לנו לחשוב איך לוקחים תיאוריה מודיעינית ומשיתים אותה על עולם הסייבר ועל העולם של רציפות עסקית פיזית. ההבדל העיקרי בין העולם הפיזי לעולם הסייבר הוא קבועי הזמן.

חוסר הוודאות שקיים בשני העולמות (הקיברנטי והפיזי) גורם לאנשים לקבל החלטות שגויות שמבוססות על זיופים או על פעולות שמבוצעות מתוך כוונות זדוניות, כמו למשל תגובה להודעה שנראית לגיטימית מגורמים כמו ביטוח לאומי. הדבר בא לידי ביטוי בעלייה חדה ברישומי הדומיינים שמתחזים להיות גופים לגיטימיים (כמו למשל זום, גופים שעוסקים במחלה, גופים ממשלתיים, בתי חולים וכיו״ב).

מגמה נוספת, היא ניצול חוסר הוודאות על מנת להתחזות אחד לשני. למשל, גורמי מדינה שמתחזים לגורמי פשיעה או לגורמי מדינה אחרת. זה מקשה מאוד על השיוך. זה אף מייתר את המודלים של המלחמה המודיעינית הקלאסיים, כי אנחנו לא יודעים לזהות אפילו איפה ומי האויב.

ניתן לבצע הקבלה בין העולם הרפואי לעולם ההגנה בסייבר. בין מאפייני הפעולה של ה- CERT בתקופת הקורונה-

א. First aid to contain- יש את יוזמת **ה-first aid** שמרכזת את כל האינדיקציות מהמגזר העסקי בנוגע לפעילות סייבר זדונית, דבר שמאפשר לזהות ולהתחיל לטפל בהקדם.
ב. Scan to detect- במקביל לתגובתיות, המטרה היא להיות **אקטיביים, לאבחן ולהתריע מראש** על פוטנציאל לפעילות זדונית, בעיקר על ידי זיהוי פרצות והתרעה לגביהן.
ג. Share to vaccine - שלב השלישי הוא **חיסון** באמצעות הגברת המודעות, cybernet שהיא רשת להפצת מודיעין איומים וכיו״ב.
ד. אמון! ספציפית כאשר ה-CERT מזהה בעייתיות עם רשתות VPN. מקווים להתריע מראש, וכשלא מספיקים נותנים את המידע לאחר מכן. **המטרה היא לייצר אמון בין מערך הסייבר לבין המגזר הפרטי.**

סנז ישר – אנליסטית סייבר ראשית ומרכזת תחום המחקר ומודיעין סייבר ב-FireEye ישראל

יש שני סוגים של מגיפות בעת הנוכחית- המגפה הביולוגית והמגפה של תקיפות סייבר- שמתפתחת מאוד בתקופה הקורונה.

הסיכונים (עבור הצד המגן) וההזדמנויות (עבור הצד התוקף) - עובדים יותר מהבית (כלומר שטח תקיפה גדול יותר לאויב) ; אפליקציות מעקב ממשלתיות (ומנגד התחזות לגורמים ממשלתיים או תקיפה שלהן) ; משבר כלכלי עולה (וממול ניצול כלכלי של אנשים במצוקה כלכלית).

המוטיבציה של ממשלות לפתור את המשבר הבריאותי גורמת להן להשקיע במו״פ, בתעשיית התרופות ובהשגת ציוד רפואי. אנחנו מכירים מספר מדינות (סין, רוסיה, איראן ונוספות) שמנסות לנצל את המצב על מנת להשיג את ההישגים שצוינו קודם. לעיתים התקיפות האלה משויכות למדינה מסוימת ולעיתים לא, משיקולים שונים. בין היתר, תוקפים מדענים ב-WHO ; תוקפים לצורכי ריגול את סין על מנת להשיג מידע שסין מסתירה ; תוקפים מכוני מחקר ופיתוח במדינות אחרות ; וכיו״ב.

החלק השני הוא מוטיבציה פוליטית- ערעור יציבות שלטון. הקורונה יכולה להפיל ממשלות, ולכן ממשלות מפתחות כלים לייצוב שלטונן. למשל- מעקב אחר מדינות אויבות, מעקב המוני אחר הציבור וכיו״ב. דוגמה לכך היא התקיפה של מספר מרכזים רפואיים גדולים בפראג, כפי שציין דניאל ראקוב, סביב הורדת הפסל התומך בנראטיב הרוסי.

במקביל לדברים שמדינות עושות, אנחנו רואים גם עלייה בפשיעה, למשל בכופרות ובפישינג.

בשורה התחתונה- גם בתחום הגנת הסייבר הקורונה שינתה במהירות את פני הדברים, וזה ייאלץ היערכות מחודשת הן ברמה המדינתית והן ברמה האישית. הכרה ברכיבי השינוי, בין היתר כפי שתוארו כאן, היא השלב הראשון, ומכאן יש לבצע היערכות, השתנות והתאמות.

אוהד זיידנברג – מייסד CTI League, וחוקר מודיעין סייבר בכיר ב-ClearSky Cyber Security

במסגרת תפקידו, הוא מעורה בנעשה בעולם הסייבר. בחודשים האחרונים, הוא ועמיתיו ראו יותר ויותר התקפות ופעולות זדוניות בעולם הסייבר נגד מערכות בריאות שמבוצעות בחסות הקורונה או לכאורה בשם המאבק בה.

זה לא דבר חדש. עולם הכוונות הזדוניות בסייבר הוא עולם מתפתח תדיר. עם זאת, בתקופת הקורונה, יש חשש שהתקפות הסייבר יכוונו לבתי חולים ולעוסקים בבריאות. הסכנה הייתה שמשאבים יושקעו בהתמודדות עם ההתקפות האלה במקום להיות מושקעים בבריאות (רכישת ציוד רפואי, שעות עבודה וכיו״ב).

לאור זאת הוקמה קהילה גלובלית של אנשי הגנת סייבר, בשם CTI LEAGUE. הקהילה שואפת לספק שירותים לבתי חולים. לאחר ההתקפה על בית החולים בצ׳כיה, הקהילה נהיית פעילה והתרחבה וכוללת יותר מ-1500 חברים ביותר מ-80 מדינות. אנשים וגופים, מומחים בסייבר, מכל העולם וללא שיוך למדינה מסוימת, שמסייעים ללא כוונות רווח לגופי בריאות. למעשה, באופן כמעט פרדוקסלי, הקורונה אפשרה לשבור את החומות של הפוליטיקה ושל הלאומיות על מנת לתמוך באינטרס המשותף של הגנה על הבריאות- שהוא אינטרס גלובלי ומחבר.

דוגמאות לפעילות- גילוי חולשות במערכות הגנה בסייבר של מערכות רפואיות ודיווח עליהן ; שיח עם נציגים מרשויות חוק שיש להן סמכות ויכולת לפעול על מנת לסכל התקפות זדוניות ; צוותי חשיבה בנוגע להמשך הפעילות של הקהילה (כאמור, הקהילה היא גלובלית ולא מוגבלת לאינטרס מדיני לוקאלי כזה או אחר) ; התרחבות מהתמקדות בבתי חולים למערכות בריאות באופן כללי (מתוך הבנה של הפגיעות שלהן) ; שיתוף מידע ושיטות פעולה על בסיס הידע המצטבר של הקהילה ; נטרול קמפיינים של דיסאינפורמציה ; וכיו״ב. למעשה, הרציונל הוא לעבוד על כל השלבים- למנוע, לטפל ולנטרל.

הקמת הקהילה פותחת דלת לשיתופי פעולה עתידיים פרו-בונו שמתכנסים סביב אינטרס גלובלי ומבטלים הלכה למעשה גבולות רעיוניים ופיזיים.