Experis Cyber: הגנת סייבר כשירות מנוהל

לאט, אבל בעיקשות של גזירת גורל בטרגדיה יוונית, הולכת ומשתרשת בעולם מערכות המידע תחושה של אסון מתקרב בדמות מלחמת הכל בכל במרחב הסייבר. מה שהתחיל כקמפיין התראות מפני שאננות יתר ואמונה מטופשת ש"לנו זה לא יקרה", הופך לנוכח עינינו ממש למועקה פרנואידית של ממש. חברות וארגונים שמים פרויקטים חשובים, שאמורים להקפיץ את איכות השרותים שהם מספקים בצורה דרמטית, על "אש קטנה" עד שיתברר אם סיכוני הסייבר הכרוכים בשינוי ניתנים בכלל לשליטה. מצב זה, נוגד פרודוקטיביות וחונק התפתחות, מהווה סיכון גדול יותר לעתיד מאשר עצם התעצמות סיכוני הסייבר. חברות שרוצות לשרוד לאורך זמן חייבות להסתגל לעבודה בעולם מסוכן בלי להסתגר מאחורי חומות פיזיות. "זו רק שאלה של תיעדוף וידע איך הופכים עקרונות למציאות בטוחה", אומר אלי כהן, מנכ"ל Experis Cyber, חברת מומחי הסייבר של חברת ה-IT הגלובלית Experis מקבוצת ManpowerGroup Israel.

"חברת הגנת הסייבר של חברת ה-IT הגלובאלית Experis".

הכמות יצאה מכלל שליטה

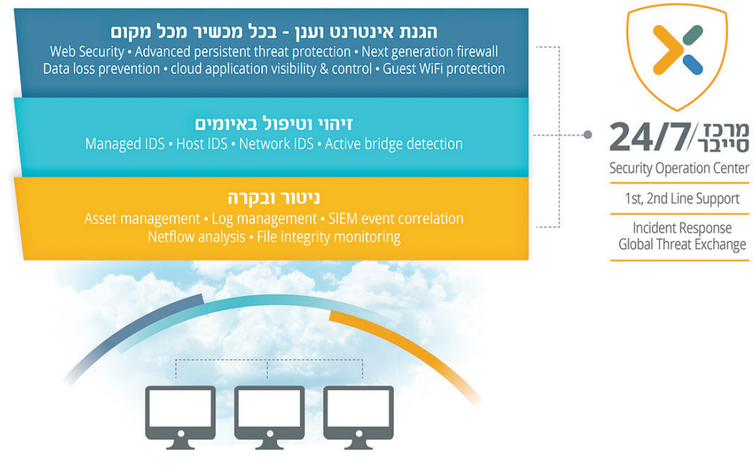
הבעיה המהותית של הגנת סייבר היא שלא מדובר ביישום פתרון אחד, או אפילו בחבילת יישומים שמעבירה את הארגון ממצב סכנה למצב בטוח. "אין פתרון 'זבנג וגמרנו', אומר אלי כהן, "מערך הגנה שמתאים לארגון אחד אינו מספק ביטחון לארגון אחר, שיש לו רגישויות אחרות ואויבים שונים. אין גם פתרון שלא מאבד מכוחו עם הזמן, שלא דורש עדכונים בלתי פוסקים, שמסוגל להתמודד עם תוכנות הזדון (Malware) החדשות, שיצוצו בעולם המקוון מחר או בעוד שנה". אימוי הסייבר מתרבים בקצב המטורף של מיליון בכל יום. במהלך 2015 נוספו לארסנל ההאקרים לא פחות מ-317 מיליון כלי תקיפה מקוונת – הרבה יותר ממספר כלי הנשק הפיזיים שמצאו את דרכם לידיים קרימינליות. האקרים הפכו להיות מתוחכמים ביותר, ויחד עם טכנולוגיות קוד פתוח ההתקפות הפכו להיות מורכבות מאוד למניעה, והכמויות יצאו מכלל שליטה. ארגונים בכל המגזרים צריכים להיערך לפעולת מניעה והתאוששות בקנה מידה מסיבי, מעבר לכדאיות הכלכלית של פיתוח יכולות הגנה עצמית. זה אתגר שיכול למצוא את המענה רק בחברות מתמחות, המשתמשות בידע ובאנשים שלהן כדי לספק שירות למספר גדול של לקוחות במודל של שרות הגנת סייבר מנוהל כמקובל בכל העולם.

"Experis Cyber היא החברה היחידה בישראל המציעה שירות הגנת סייבר במודל חדשני של שלוש השכבות הכולל הגנה תוך ארגונית, זיהוי אימומים והגנת אינטרנט מלאה לחברות מסחריות וארגונים גדולים", אומר אלי כהן, "אנחנו מונחים מרצון על ידי מטה הסייבר הלאומי ונמצאים בקשר רציף עם אנשי המטה לגבי השירותים והטכנולוגיות שאנחנו מציעים. העברת הטיפול באימוי סייבר לאחריות Experis Cyber יכולה לחסוך לגוף עסקי בין 40 ל-60 אחוז מעלויות הבעלות הכוללות. יתר על כן, הלקוח מדלג על התקופה הארוכה של לימוד, ניסוי וטעיה, שמשמעותה פריצות ונזקים בלתי חוזרים. כהן מוסיף, 70% מהמנכ"לים של החברות בארצות הברית מזהים את נושא איום התקפות הסייבר כדבר ההרסני ביותר שיכול לפגוע בחברה. בישראל לא רק הממון והמשאבים חסרים ליכולת הגנה אפקטיבית לארגונם. מנכ"לי החברות מתחילים להבין כי הסייבר הוא שירות שאמור לעטוף את ליבת העסקים. אך מכיוון והם צריכים לדאוג לרווחיות של החברות, הם אינם יכולים או צריכים להתעסק ברמה היומיומית בהגנה אקטיבית על מערכות המחשוב. במציאות שנוצרה, הפתרון שלנו הוא היעיל והאפקטיבי ביותר. בסופו של דבר, הבנה של חשיבות התפקיד שימלא הגנת הסייבר בעתיד הקרוב בעולם העסקי והלאומי ושחרור התפיסות הישנות היא המפתח".

שרות עוטף במקום הטמעת מוצרים. מה קורה בעולם?

אנליסטים וחוקרים באקדמיה מצאו שלמעלה משליש מתקציבי הסייבר מכוונים לרכישת שירותי הגנת סייבר מנוהלים, וכי החלק הזה הולך וגדל ככל שהתחום נעשה מתמחה יותר. בישראל אנו עדיין בתחילת הדרך, והרבה חברות מהססות להוציא שירותי ליבה חיוניים למיקור חוץ, ואבטחת סייבר נתפסת כסוגיה שחייבים להתמודד איתה בתוך הארגון. "ב- 15 שנה האחרונות התפיסה הייתה של הטמעת מוצרים, אולם אפשר לומר עכשיו בפה מלא שהתפיסה הזו אבד עליה הכלח. השקיעו מיליונים אבל הארגונים פרוצים, המומנטום של הרציונל העסקי מתחיל להתגבר על השמרנות, במיוחד לאחר שהגישה המסורתית - לעשות הכל לבד - פשוט לא עומדת במבחן התוצאה".

לא הרבה ארגונים מוכנים לשתף את הציבור במידע על התקפות סייבר שהם חוו ובוודאי שכולם מנסים להעלים אירועי תקיפה שהצליחו. "למי שרחוק מהקלחת נדמה שהמצב תחת שליטה", אומר אלי כהן, "אבל הסטטיסטיקה ממש לא מרגיעה. 5 מתוך 6 חברות, הותקפו בשנה האחרונה. במתקפות סחיטה (Ransomware), בהן ההאקר משבית את מערכת המידע של הגוף המותקף עד לקבלת כופר, נרשם גידול של 113 אחוז. התקפות על גופים ממשלתיים, ממניעים של טרור פוליטי או חבלנות מדינתית, גדלו ב-90 אחוז. נכון, הגל של מתקפות וירוסים מתחיל לעבור, אבל מה שמגיע במקומו הרבה יותר מסוכן. Advanced Persistent Threat (או בקיצור APT) הוא איום מורכב המטמיע מספר אמצעי תקיפה משולבים עם יכולת לתקוף בהסתר לאורך זמן ולהימנע מגילוי. לפעמים נדרשים שלושה, ארבעה חודשים כדי לזהות את ההתקפה, לנטרל את כל מרכיביה ושלוחותיהם במערכות שונות, לטהר את הרשת הארגונית מכל בדל קוד זדוני ולהפעיל את כלי ההגנה שימנעו הדבקה חוזרת. כמה גדול הנזק מהתקפה שהצליחה? באר"ב מוערכת העלות הממוצעת לארגון מסחרי מתוצאות פריצה אחת ב-4 מיליון דולר. ואנו לא מדברים על פריצות ספקטקולריות, כמו זו שהתרחשה ב-Sony, שיכולות לרסק את שווי החברה במיליארדים רבים".



חברת סייבר גלובלית ומודל שלוש השכבות

אם המותג Experis Cyber נשמע חדש ואתם שואלים את עצמכם איפה הסתתרו השירותים והמומחים האלה עד היום, כדאי להביט לרגע אחורה ולראות מהיכן הם הגיעו. עד סוף 2015 החברה פעלה תחת השם ConnectIT בעצמאות גמורה. התרחבותה של Experis Israel לתחומי הסייבר, והמגע השוטף עם מגמות חדשות מחו"ל הביא לריכוז כל הפעילות במסגרת שירותי הגנת סייבר תחת המותג Experis Cyber, שהפכה בעצם לזרוע הסייבר הישראלית של חברת EXPERIS העולמית, אחת המעסיקות הגדולות בעולם של מומחים ושל פתרונות עסקיים - בתחום ה-IT. מדובר ביותר מ-38,000 עובדים, ביותר מ-50 מדינות ברחבי העולם בנושא אבטחת סייבר והגנת מידע. החברה פיתחה מודל הגנה מודולרי של 3 שכבות המשלימות אחת את השניה אולם הן בהחלט מודולריות ויכולות להיות מיושמות בשלבים. כל אחת מהשכבות מחוברת אל מרכז התמיכה המשוכלל של החברה המאוכלס סביב השעון על ידי מומחי סייבר ואנליסטים שמנתחים את אירועי אבטחת המידע של הלקוחות ופועלים מידית לעצירת אימומים.

שכבת ניטור ובקרה (מערכות SIEM גלובליות): הכוללת מניעת דליפות מידע, עצירת סוסים טרויאניים וגניבת זהויות. המערכת נפרסת תוך ימים ספורים ומאפשרת לנטר שרתים, עמדות קצה ותנועת רשת, ובעזרת תהליכי אנליזה מתקדמים מוציאה התראות אבטחת מידע מדויקות. המערכות מחוברות למרכז הבקרה שלנו אשר מאפשר מתן פתרון וניתוח של האירוע ללקוחות.

שכבת זיהוי וטיפול באימומים: מדובר בשכבת הגנה הכוללת כלים טכנולוגים מתקדמים שחלקם פותחו בישראל לזיהוי אימומים מתקדמים. "התפקיד שלנו, כנותני שרותי הגנה, הוא לשדרג את הטכנולוגיה ואת תהליכי העבודה על מנת לעמוד בקצב האימומים המהיר". סוגים שונים של Botnets, malware, virus נוצרים כל הזמן, ואנו רואים כיצד מדובר במשחק של חתול ועכבר, כאשר עלינו, כספקי שרות הגנה, מוטל להיות צעד אחד לפני פושעי הסייבר ולכן אנו דואגים לשיפור מתמיד בטכנולוגיה, בתהליכי העבודה ובמומחים שלנו.

שכבת הגנת האינטרנט: בעזרת פתרונות טכנולוגיים של שותפים עסקיים אנו מספקים ללקוחות שלנו פתרון גלובלי, לכל סוג של מכשיר (נייד, מחשב נישא, טבלט) בכ- 100 מרכזי שירות בעולם, כל אחד כולל Data Center וצוות מומחים רב-תחומי לתמיכה בלקוחות גלובליים. הרשת העולמית מספקת מספר עצום של נקודות ניטור, אמצעי ניתוח אימומים, סריקת מערכות והפעלת התראות מרחוק. "אם באבטחה קונבנציונלית אומרים שחוזק השרשרת הוא כחוזק החוליה החלשה ביותר, בהגנת סייבר אנו אומרים, שחוזק החומה הוא כחוזק המצרפי של המשאבים שפיזרנו בכל העולם".

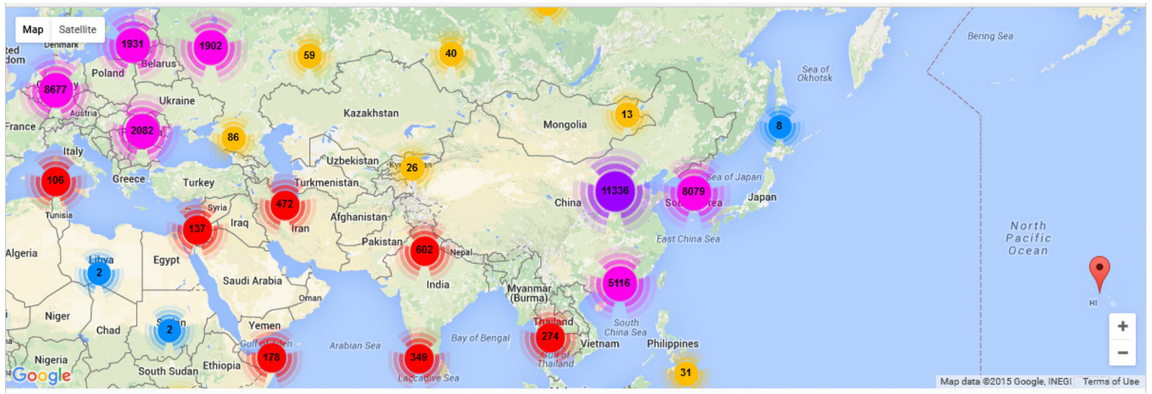
זרימת ידע דו כיוונית

המומחים של Experis Cyber לא רק מביאים לישראל את המתודות, הכלים ונגישות של המומחים העולמיים של Experis, אלא גם מזיינים ידע ישראלי למערכת הגלובלית. "מדובר בקשר דו-צדדי", אומר אלי כהן, "למומחים הישראליים מוניטין בכל העולם, במיוחד אלה מהם שלמדו ורכשו ניסיון במערכות הגנת סייבר של כמה מהגופים השמורים ביותר בישראל. אלה עושים את המומחיות של אנשי Experis Cyber לסמכות מקצועית מוערכת הרבה מעבר לגבולות ישראל. ומצד שני, הקשרים העולמיים עוזרים לייבא לישראל ידע מעשי מארה"ב ומאירופה. למשל, מנהל ציות לרגולציה פיננסית ותקנות הבנק הפרטיות, ניהול סיכוני ושליטות תאגידית. החברה שלנו לא מנסה להחליף את היועצים העסקיים והמשפטיים במומחי IT, אבל כידוע מדובר בנושאים טכניים שמחייבים מערכות מוגנות היטב. בנוסף להוכחת החוסן מול סיכונים חיצוניים ופעילות חבלנית מבית, הרגולטור דורש שניתן יהיה לחקור כל אירוע לעומקו ולתעד את השתלשלות המאורעות צעד אחר צעד. מדיניות GRC ברורה, עם כלים חזקים ל-Audit חודרני, היא הפן השני של הגנת סייבר אפקטיבית. התפיסה המשולבת הזאת מגיעה מחו"ל, ממאות חברות Enterprise שנתנו למומחי Experis לנהל את המערכות הארגוניות במיקור חוץ, ומעשירה את השירותים שלנו בישראל בערך מוסף ייחודי".

מחויבות בלבדית לטובת הלקוח

הארגון מחדש של Experis Cyber משקף מגמה עולמית של הפרדה בין חברות מוצרים - מפתחות ומפיצות - לבין חברות מומחיות שירות ויישום. המורכבות ההולכת וגדלה בעולם היישומים הארגוניים, ולא רק בתחום הגנת הסייבר, יוצרת מצב פוטנציאלי של ניגוד אינטרסים בין שני הצדדים. יצרני מוצרים מעוניינים למכור את מרכולתם ועבורם מדובר ב"משחק סכום אפס". "אם המתחרים שלי מוכרים את זה, זה מוצר שאני לא יכול למכור", אומרת צורת החשיבה של חברות מוצרים. לעומת זאת, עבור חברת שירותי הגנת סייבר, האיכות היא שם המשחק כאשר כל מוצר שמשפר את איכות השירות, גם אם הוא מוריד עלויות ומקטין את היקף החוזה, ראוי שיכנס לסל ויתחרה על חלקו. במעבר מהמותג ConnectIT ל- Experis Cyber הכריעה הנהלת Experis שהעתיד הוא באספקת שירותי מומחים נטו על בסיס הטכנולוגיות המתקדמות בעולם.

מטרית הגנה ללא גבולות

ברמה הגלובלית Experis Cyber מחויבת לחזון של חברת האם, "עולם בלי גבולות". כפי שההאקרים לא מתחשבים בגבולות והעסקים מנסים לנצל הזדמנויות גלובליות בכל הפעילויות הארגוניות - החל בניהול שרשרת אספקה עולמית וכלה בפיתוח ערוץ שיווק מקוון חובק עולם - גם תשתיות ה-IT אמורות לתפקד כשירותים חוצי גבולות. "משתמש ישראלי בחברה שמקבלת שירותי אבטחה מ-Experis יקבל מטריית הגנה שהולכת איתו לכל מקום בעולם", אומר אלי כהן. "הגנת סייבר אינה נגמרת במשרד ואפילו לא באולם היוצאים בנתב"ג. מערך ההגנות עוטף את המשתמש הנייד כמו ענן וירטואלי, שומר על המכשירים הניידים מסכנות החיבור ל-Web בכל מקום שנוצר קשר בין המחשב הנייד, הטאבלט או הסמארטפון עם האינטרנט".

"לעולם לא נשכח שנקודת הקצה המשוטטת בעולם היא נקודת חדירה אפשרית למערכת הליבה, שנשארה ב-Data Center בבית. פעם, לפני שפותחו הפתרונות שמאפשרים להקיף את המשתמש הנייד בהגנות ניידות בכל מקום שימצא, גופים רבים המודעים לסכנות הסייבר אסרו על הוצאת מחשבים או אבזרי אחסון מהמתחם הפיזי של המשרדים. אפילו שירותי דואר הופרדו פיזית ממערכות היצור ועובד שיצא מהמשרד נותק למעשה מכל קשר לתכנים דיגיטליים. ברור שמגבלות כאלה פוגעות קשה בזרימת העבודה, בתפוקות האישיות ובמוטיבציה לנצל כל רגע לקידום יעדי הארגון. כיום אנחנו יכולים להגמיש את תנאי הבידוד בלי לפגוע בביטחון. יותר ויותר ארגונים, גם כאלה שמסוגלים לתחזק חומת אש בלתי חדירה כל עוד מדובר בפריסה ארצית, מעיגים אלינו לקבל שירות הגנה חובק עולם. מסיבות ברורות אני לא רשאי לפרט ולזהות את הלקוחות האלה, אבל דבר אחד אני יכול להגיד בהקשר זה: מה שטוב ללקוח ברובד הביטחון הלאומי, יותר ממספיק לשוק ה-Enterprise העסקי. שירותי הגנת הסייבר של Experis Cyber יגנו עליכם טוב יותר בלי להשקיע הון עתק בתשתיות - ותוכלו בהזדמנות זו גם להוריד עלויות שוטפות בעשרות אחוזים".