חברת Q.rity
חומת המגן של הרשויות המקומיות מפני מתקפת סייבר

Q.rity מקבוצת TSG מספקת היום לרשויות מקומיות את האבטחה הנדרשת מול כל איום סייבר. החברה פיתחה מרכז ניטור חכם, מותאם לצרכים של כל רשות, אותו מפעיל צוות מיומן שיודע להתערב בעת הצורך ומעניק שקט נפשי לכל מנהל אבטחת מידע ברשויות המקומיות.

מיכאל זינדרמן, מנכ"ל TSG

כל מנהל אבטחת מידע בחברה פוגש במהלך עבודתו טכנולוגיות רבות המוצעות לו על מנת להתמודד מול איומי התקפות סייבר. אתגרם המרכזי של העוסקים בתחום הוא להילחם בלא נודע, כיוון שלא ניתן לזהות מראש מהו הנזק שיכול להיגרם ממתקפת סייבר.

בעבר התמודדנו מול מערך כלים ידוע, כמו וירוס בעל חתימה, או כלי תקיפה שניתן ללמוד עליו מבעוד מועד. אולם כיום, בעידן בו המתקפות ממוקדות והיעדים ברורים ומדויקים, אי אפשר לסמוך שתהיה הכרה מראש של אופי התקיפה.

לכן, ניטור הרשת בצורה חכמה וביצוע הצלבות בין פריטי מידע רבים ושונים, בשילוב מודיעין איכותי, הפכו להיות הכלי הנכון לזיהוי מתקפה פוטנציאלית וניסיונות חדירה עוד לפני שהרשות המקומית חוותה שיבוש תהליכי עבודה, או חלילה איבוד מידע.

בשל כניסת הטכנולוגיה למגוון שירותים הניתנים על ידי הרשויות המקומיות, הן הפכו להיות אחראיות על שמירת מידע רגיש, הכולל פרטים אישיים רבים של התושבים. וככל שהאחריות גדולה יותר, כך האופציה והמוטיבציה לפגוע ברשות גבוהות יותר.

להתקפות סייבר יכולה להיות השפעה תדמיתית וכלכלית עצומה על רשויות מקומיות. כל טעות קטנה שנובעת מאי מוכנות, יכולה לחשוף מאגר מידע אישי רגיש של תושבי הרשות. מעבר להפסדים הכספיים שיכולים להיווצר, ייפגע גם אמון הציבור ברשות וביכולת שלה לספק שירותים חיוניים בצורה מקוונת ורציפה.

הפתרון לאיום הסייבר על עיריות נמצא במרכז הניטור CSC של Q.rity

"חלק מהרשויות המקומיות בישראל אינן ערוכות להתמודד עם מתקפות סייבר. הרשות להגנת הפרטיות, מערך הסייבר ומשרד הפנים נוקטים בפעולות, אך אין בכך לסייע או לתת מענה מספק למכלול הסיכונים". כך כותב מבקר המדינה, מתניה אנגלמן, בפרק על ערים חכמות ורשויות מקומיות בדו"ח מבקר המדינה שהתפרסם בשנת 2020.

דוגמאות מהעת האחרונה פורסמו בהרחבה בעיתונות, כמו השרת של מחלקת ההנדסה בעירייה בצפון הארץ שהותקף והדבר גרם לכך שחלק גדול מהמידע נחסם בפני העירייה. כתוצאה מכך, לא הוגשו על ידה כתבי אישום נגד עברייני בנייה. במקרה אחר האקרים פלסטינים הצליחו לפרוץ לשרתי עירייה במרכז הארץ ולגנוב משם שמות משתמש וסיסמאות של עובדים. מניעת מקרים כאלה הם במיקוד העשייה של Q.rity .

חברת Q.rity, מקבוצת TSG - חברה בבעלות התעשייה האווירית ופורמולה מערכות, מציעה חבילת שירותים המותאמת לאתגרי הסייבר החדשים ברשויות המקומיות. אחד השירותים המשמעותיים והחשובים הינו מרכז ניטור סייבר - CSC (Cyber Security Center) הפועל סביב השעון.

המודל העסקי של המרכז, מאפשר לרשויות המקומיות להתמודד עם הסכנות באופן נקודתי במקום להשקיע משאבים עצומים של כסף וזמן באבטחת הסייבר פנים ארגונית. העלות של הפעלת מרכז ניטור חיצוני הוא זניח לעומת עלות הפגיעה כתוצאה ממתקפת סייבר אם חלילה תתרחש.

ה-CSC פועל לאורך כל שעות היממה ומנטר ארגונים מהארץ ומהעולם, הנמנים עם לקוחות הקבוצה. המרכז משתמש בטכנולוגיות המתקדמות ביותר בתחום ומפעיל צוות מומחים בעלי ניסיון רב בעולם הסייבר.

ישנן שתי מטרות מרכזיות בפעילות מרכזי הניטור: הראשון הוא לשמש כמרכז בקרה הבוחן קשרים בין מקורות מידע שונים, בשילוב של מודיעין איכותי המסייע להבנה טובה יותר של האיומים הצפויים. השני הוא להפעיל מודיעין ולחפש התנהגויות וממצאים חשודים ברשת, עוד לפני שישנה התראה או אירוע סייבר. הפעילות הפרו-אקטיבית של החוקרים במרכז מהווה מכפיל כח והסתכלות רחבה ועמוקה על הרשת.

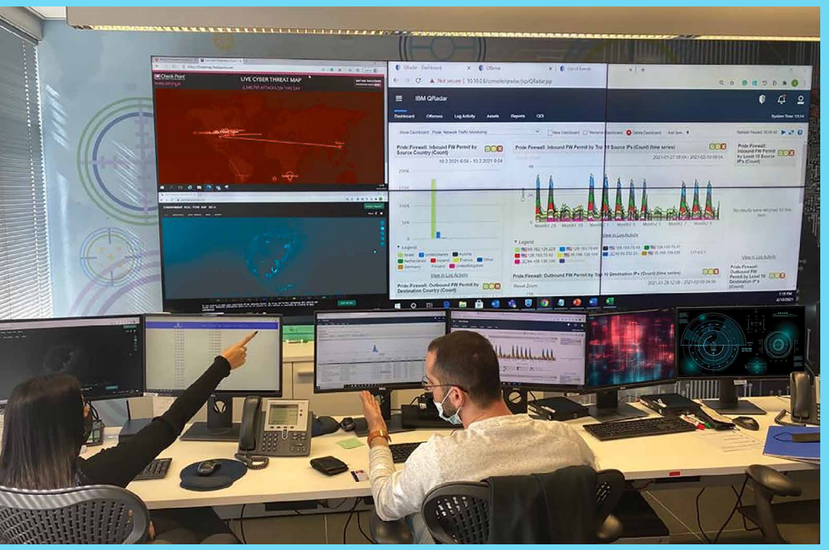
Q.rity מספקת הגנה לרשויות מקומיות גם בימי הקורונה

בין הלקוחות של Qrity ניתן למצוא רשויות מקומיות גדולות שבחרו לאפשר לאנשי ה-IT בעיריה להתפנות ולעסוק בתחומם. אלו מקבלים שירותי הגנת סייבר מותאמים לפי צרכים, החל מהערכת סיכונים, ניטור שוטף, מודיעין סייבר איכותי, ואפילו צוות התערבות זמין בעת הצורך, אשר מלווה את מנהל אבטחת המידע בעירייה.

בגלל מגיפת הקורונה, יש יותר עבודה מהבית. זו מציאות שיוצרת מצד אחד שינויים מהותיים מבחינת פריסת ה-IT בארגון, עובדה אשר חושפת את העיריה לאיומי סייבר חדשים. רשויות מקומיות רבות פועלות כיום במודל עבודה שונה שהמעבר אליו התרחש בתוך תקופה קצרה מאוד, ולכן קיים קושי להיערך לשינוי כזה בהתאם. כך למשל, העובדים נעזרים במחשבים אישיים שנמצאים בבתים ושבאופן טבעי לא מוגנים בחבילת הגנת סייבר מעודכנת. סגנון זה של עבודה יוצר מרחב איומים שונה ורחב יותר. CSC נערך למתן שירותים חדשים, משלימים ומותאמים למצב זה, ומספק ללקוחות מגוון שירותים ממוקדים כדי להתמודד עם האיומים החדשים.

המרכז החדשני של Q.rity ממוקם בפארק הסייבר בבאר שבע, באקו-סיסטם המשלב את כל חברות הסייבר המובילות מצד אחד, ואת אוניברסיטת באר שבע בתחום המחקר מהצד השני. עובדי Q.rity מתרגלים מדי יום התמודדות עם מתקפות סייבר מסוגים שונים ונחשפים למגוון אירועי סייבר בקנה מידה גדול. יש להם את המומחיות, הכישורים והידע הנדרש להגנה על כל רשות מקומית, בלי קשר לגודלה.

לפרטים נוספים ויצירת קשר עם Q.rity:
sharon.abekasis@qritys.com



מרכז הגנת הסייבר CSC של Q.rity בבאר שבע