שירותי אבטחת סייבר מנוהלים

פלטפורמת הגנת סייבר

ניהול תקריות סייבר

ייעוץ ותקינה

Simplifying Security

BYNET CYBER-DOME

תקשורת מחשבים בע"מ

איומי הסייבר בעולם הפוסט מודרני

פושעים מאורגנים, האקטיביסטים (Hacktivists) ואף סוכנים של מדינות אויב משיקים מתקפות סייבר בלתי פוסקות, ולעיתים בעלות פרופיל תקשורתי גבוה, כנגד ארגונים מסחריים, גופים ממשלתיים ואפילו תשתיות מדינתיות קריטיות.

עובדה זו העלתה את המודעות לתחום אבטחת המידע והסייבר, ונתנה תחושת דחיפות לצורך בהגנה על המידע הקריטי לארגון מפני גניבה והפצה בשוק השחור של הרשת האפלה (Dark Web).

קניין רוחני, סודות מסחריים, מספרי כרטיסי אשראי והסכמי עבודה חסויים הם מטרות רווחיות ביותר עבור עברייני הסייבר, עם פוטנציאל לגרימת נזקים אדירים לארגון המותקף ואולי אף לקריסתו. כל מידע אשר נגנב מארגון עלול להוות בסיס למתקפות נוספות המתבססות על זהות גנובה, ובכך לחשוף את הארגון לתביעות ולנזק נוסף.

התוקפים של ימינו מתוחכמים יותר, מצויידים בטכנולוגיה טובה יותר ומכווני מטרה הרבה יותר מבעבר. כאשר לעובדות אלה מתווספת המציאות המודרנית שבה כל ארגון עסקי נדרש להיות מחובר לרשת - התוצאה העגומה היא שכל ארגון חשוף לפריצה, או שאולי כבר נפרץ ואינו מודע לכך.

הטכנולוגיה מתקדמת, התוקפים יותר

פתרונות הגנת הסייבר כיום אינם מספקים, ונדרש שינוי גישה

תחום אבטחת המידע והסייבר מונע, כמו תחומים רבים אחרים, מהשילוב בין אנשים, טכנולוגיה ומדיניות. באם השילוב והאינטגרציה בין רכיבים אלה הוא מוצלח בארגון - אבטחת המידע הארגוני מובטחת.

לב ליבו של תהליך שילוב שלושת האלמנטים הללו יחדיו בצורה אפקטיבית הינו אלמנט האנשים. אלמנט זה בדרך כלל אינו מטופל בצורה נכונה בארגונים, הן בשל חוסר במשאב ייעודי ומקצועי המטפל בנושא והן בשל חוסר מודעות של עובדי הארגון וספקים חיצוניים העובדים עם הארגון.

איומי הסייבר המודרניים אינם גזירת גורל, וניתן להתגבר עליהם על ידי יישום מספר עקרונות בתכנון ארכיטקטורת אבטחת המידע הארגונית:

- משאב ייעודי ומקצועי אשר מרכז את נושא אבטחת המידע בארגון
- הגדרת ארכיטקטורה ברורה ומלאה, המשלבת את צרכי הארגון הן מבחינה עסקית והן טכנולוגית
- חינוך עובדי הארגון ומשתמשים חיצוניים לארגון לאבטחת מידע נאותה
- שימוש בטכנולוגייה איכותית ואפקטיבית

שירותי אבטחת מידע וסייבר

אתגרי איומי הסייבר המודרניים על ארגונים ידועים מזה מספר שנים, ואנו עדים לעלייה תלולה במספר תקריות אבטחת המידע ודלף המידע מארגונים שונים תוך גרימת נזק ניכר לארגונים השונים. בשל כך, קיימת מגמה מתמדת ומתחזקת של ארגונים למעבר לשירותי אבטחת מידע וסייבר מנוהלים. מגמה זו מתחזקת כתוצאה מההבנה שנדרשת מומחיות ומקצועיות ייחודית וייעודית על מנת למנוע את התקיפות המודרניות, מומחיות אשר אינה קיימת ואינה יכולה להתקיים ברוב הארגונים.

שירותי אבטחת סייבר מנוהלים

Bynet Cyber-Dome הינו שירות מנוהל עבור כל צרכי אבטחת המידע והסייבר הארגוניים. השירות כולל שילוב ייחודי של פלטפורמת הגנת הסייבר Cyber-Dome עם מומחי הסייבר הטובים בתעשייה אשר מנתחים ומנטרים את הרשת הארגונית באופן מתמיד.

פלטפורמת הגנת סייבר מלאה

Cyber-Dome הינה פלטפורמה להגנת סייבר אשר מיישמת מספר רב של טכנולוגיות הגנת סייבר מתקדמות תוך אינטגרציה וסינרגיה ביניהן. סינרגיה זו היא המספקת את ההגנה הייחודית, והיא זו המאפשרת למומחי הסייבר המתפעלים את המערכת להגיב באפקטיביות ובמהירות לכל איום סייבר ולמנעו.

ניהול תקריות סייבר

נדבך חשוב בתחום הגנת הסייבר המודרנית הוא יכולת התגובה המיידית לכל איום, גם איום שכבר הספיק לחדור לרשת הארגונית. במסגרת שירות ה-Cyber-Dome קיים צוות מענה מיידי (Incident Response Team) אשר ערוך הן למענה באתר הלקוח (On-Premise) והן למענה מרחוק עבור כל אירועי סייבר שחדר לרשת הארגונית.

שירות מתקדם בשילוב פלטפורמה ייחודית

ייחודיות פתרון Bynet Cyber-Dome הינו היכולת לשלב את שלושת האלמנטים הנדרשים עבור ארכיטקטורת אבטחת מידע וסייבר נכונה - אנשים, טכנולוגיה ותהליכים. הפתרון נסמך על מומחי סייבר מהטובים בתעשייה, על פלטפורמת הגנת סייבר ייחודית ועל הנסיון הרחב ורב השנים של "בינת" בתחום הגנת הסייבר.

- מומחי סייבר מקצועיים
- פעילות פרו-אקטיבית לשיפור החסינות הארגונית להתקפות
- פריסת Cyber-Sensors ברשת הארגון לגילוי ומניעה מיידים
- שימוש בטכנולוגיות Hybrid-Cloud למימוש הפתרון האפקטיבי ביותר
- פעילות 24x7
- צוות תגובה מיידית (Incident Response Team)

האם הארגון שלך ערוך להתמודד עם איומי הסייבר?

- מתקפות סייבר ממוקדות ובלתי פוסקות על הארגון
- צרכי אבטחת המידע מגוף ה-IT הולכים וגדלים, על חשבון התמקדות בתחומים אחרים
- האיומים מורכבים ומגיעים ממקורות שונים, כאשר גבולות הארגון מיטשטשים כתוצאה משימוש באמצעי תקשורת ניידים כגון Smartphones
- גודלה ותקציבה של חטיבת ה-IT אינו מאפשר מיקוד ומשאבים ייעודיים בתחום אבטחת המידע
- מחסור במומחי סייבר מיומנים במשק
- קושי בניהול ובקרה על אמצעי האבטחה בארגון מפאת מורכבותם ומספרם

בינת
תקשורת מחשבים בע"מ

לפרטים ומידע נוסף: info@bynet.co.il | www.bynet.co.il