הגנה כוללת על נכסי הארגון\אורן ברט 2Bsecure

במהלך השנה האחרונה חלו מספר שינויים אקוטיים בעולם המידע, שינויים אלו מובילים את עולם אבטחת מערכות המידע לכיוונים חדשים כאשר את חזית עולם ההגנה כובשות מערכות ההגנה בנקודות הקצה מחד, ומאידך חלה עלייה משמעותית בצורך בהגנה על המידע, האפליקציה, ובסיסי הנתונים.

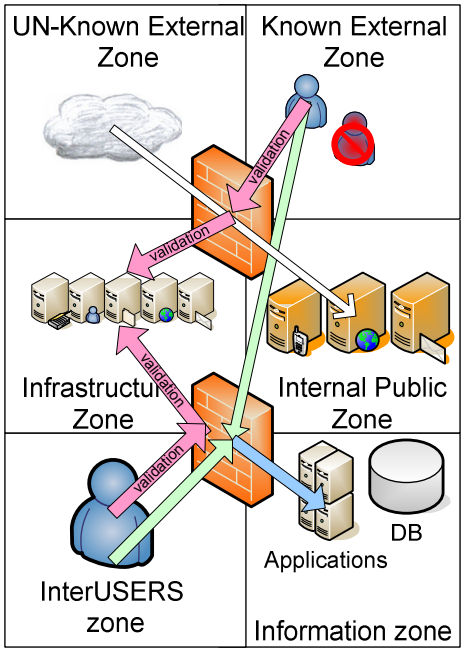
שנת 2006 התאפיינה בשינויים מז'וריים של עולם מערכות המידע, שינויים אלו מונעים בעיקר משלוש סיבות עיקריות:

1. הרגולציה הולכת ותופסת לה מקום מרכזי בשיקולי בניית המערכת כך שבעצם נקבעו מס' סטנדרטים הקובעים את תצורת מערכות המידע בארגונים הגדולים.

2. הגלובליזציה אשר התחזקה בשנה החולפת מחייבת מתן אפשרויות רבות מגוונות ופשוטות ככל הניתן לשיתוף מערכות מחד לצד ביזור של מערכות המידע הארגונית.

3. הרוויה והבשלות של מערכות ההגנה התשתיתיות (IPS,VPNs,FireWalls וכד') מהווה חסם עמיד בפני התקפות תשתית, ולמעשה בכל חלקה השני של שנת 2006 לא דווח על "זנים חדשים" של ווירוסים תשתיתיים.

שינויים אלו מהווים את הבסיס לשינוי המהותי החל בעולם הגנת מערכות המידע, המעבר מהגנה תשתית (המתבססת על אבטחת רשת המידע והמבואות אליה), להגנה על המידע והתוכן הקיים במערכות. היבט נוסף הדורש התייחסות הוא האמירה הידועה כי "**70 עד 80 אחוז מהאיום על המידע נובע מחלקה הפנימי של הרשת**" אמירה זו מוכרת וידועה אולם מפתיעה העובדה כי למעשה כמעט ולא קיימים פתרונות טכנולוגיים המאפשרים מגננה מלאה מפני "המשתמש המורשה" אשר מהווה על פי אמירה זו את האיום המרכזי. אל מול שינויים אלו מתרחשים בתקופה האחרונה מספר שינויים טכנולוגיים ותפיסתיים מהותיים.
כבר בתחילת השנה הנוכחית ניתן להבחין כי עיקר הפיתוח וההתקדמות של פתרונות האבטחה נע לכיוון של הגנת עמדות הקצה (End Point Security) מחד והגנה על רמות 3 עד 7 במודל ISO מאידך. שינויים אלו מתבטאים בכניסה של יצרני מערכות ה FireWall והAntiVirus הקלאסיים לתחום הגנת עמדות הקצה תוך יצירת מערכות ריכוזיות, מנוהלות ומעודכנות אשר מאפשרות הן להגן על תחנת העבודה גם בהיותה מחוץ לרשת הארגון והן לאפשר למנהל מערך ההגנה להתגונן מפני פעילות מאיימת הנובעת מתחנות הקצה.
מערכי ה - EPS (End Point Security) מתגבשים סביב יכולת לבצע הגנה אל מול איומים על התשתית ואפליקציה לצד הגנה מפני זליגת מידע והחדרת תכנים או פוגעני רשת על ידי המשתמש המורשה. רכיב חשוב במערכי הגנה אלו הוא מערך הניהול הריכוזי המאפשר התייחסות ברמת המשתמש, הקבוצה, הסיטואציה, המיקום המערכת וכד' –בדומה למערכות הניהול הקלאסיות בעולם ה AntiVirus .



היבט חשוב נוסף הוא התנופה שמקבל נושא הגנת בסיסי הנתונים. בסיס הנתונים הינו לב ליבו של מערך המידע הארגוני ומהווה נדבך קריטי בפעולתו התקינה של הארגון ככזה הוא מהווה מטרה מאתגרת עבור פורצים. בסיסי הנתונים מתנהגים בבסיסם כמערכות אפליקציה רשתית (WEB Applic) ומתבססים על עבודה מול מערכות תשאול המהוות בסיס חציצה בין הלקוח למערכת. מערכות ההגנה הקיימות מאפשרות לבצע פעולת בדיקה של חוקיות השאילתה, הפעולה ומבצע הפעולה תוך בחינה של התאמתם למדיניות הגישה לנתונים שהוגדרה על ידי מנהלי הנתונים. לצד כל אלו הופכת פעולת הכתיבה של האפליקציות כמעט למשימת אבטחה שכן יש לשקול את כל האיומים האפשריים הנובעים הן מהיבטי התקשורת הן

מהיבטי ה"משתמש המורשה" והן אל מול איומי התוכן המתחדשים חדשות לבקרים. כך שלמעשה נותר הליך תמידי של תכנון פיתוח בקרה ועדכון האפליקציה תוך שימת דגש על היבטי אבטחת המידע כחלק מובנה בתהליך.

לצד הפיתוחים והחידושים בתחומי הגנת משתמש הקצה, הגנת ותכנון האפליקציה ואבטחת בסיסי הנתונים חלו שינויים במבנים המסורתיים של תשתיות האבטחה, מתוך כוונה לייצר סביבות יעילות וגמישות יותר אשר יאפשרו לכל הגורמים הפעילים ברשת (מהמשתמש הפשוט ועד למנהלי המערכת מחד, ומאידך אפליקציות ושירותים) לנצל את משאבי המידע הקיימים ברשת וזאת מבלי לפגוע ברמת הביטחון של התשתית והמידע הארגוני. תפישת האבטחה החדשה מתבססת על חלוקה של הרשת לאזורי שימוש על פי מבנה הפעילות הארגוני תוך ביצוע של חציצה מבנית מלאה ומותאמת עבור כל שירות או יחידת מידע המתבססת דווקא על מערכות האבטחה כשדרת הרשת. מיקומה של מערכת האבטחה על השדרה מצריך ביצועים ואמינות רבה יותר אך מקנה למנהל התשתית את היכולת לבצע סינון יעיל ומובנה יותר של המידע הזורם ברשת הארגונית. פתרון נוסף הנובע מתצורה זו הינו היכולת להקנות רמת בטחון שווה בין משתמש הממוקם בטווח הרשת הפנימי (70 עד 80 אחוז) לבין כזה הממוקם מחוץ למערכת (פנימי או חיצוני), הגישה של **כל** הגורמים אל המידע תתאפשר אך ורק דרך מערכת בידול ותוך מעבר של כל שדרת האבטחה.

אל מול האתגרים והאיומים המתחדשים על נכסו העיקרי של הארגון **הידע** נדרשת הערכות מורכבת ומשולבת מהבנה ויכולת ניתוח של מערכות תשתית מורכבות, סביבות רשת מבוזרות ומגוונות מערכי תקשורת משולבי קול וידאו וזרימות מידע (Streaming). לצד הבנה מעמיקה בפיתוח, בסיסי נתונים והתנהגות ארגונית.יכולות אלו בשילוב הפתרונות המסורתיים ואלו המתפתחים בתקפה האחרונה מקנים למהנדס האבטחה לייצר מערכי אבטחה המותאמים יחידנית (Tailor made) לצרכים הארגוניים למערכות האפליקציה הארגוניות. ומושתתים עמוק אל תוך מדיניות הניהול והתרבות הארגונית.
חברת **2Bsecure** משתפת פעולה עם היצרנים המובילים בתחום ההגנה על עמדות הקצה וההגנה על התוכן והאפליקציה, ומשלבת יכולת ניתוח ייעוץ וסיוע בתכנון ופיתוח מאובטח של מערכות האפליקציה והתשתית.