התרחש אצלי אירוע אבטחת מידע - מה לעשות

מאת אורן שני [29/09/2008]

התרחש אצלי אירוע אבטחת מידע ? מה לעשות?בשנים האחרונות אנו רואים אחת לתקופה כי ארגון זה או אחר נפגע באירוע אבטחת מידע. בין אם גניבת מידע, תקיפת אתר הארגון, הרשת או דליפת מידע. ברוב המקרים נשמע רק על אירועים רוחביים העשויים להשפיע גם עלינו (כגון אירועי Phising בבנקים), כאשר למעשה כמות האירועים המתרחשת הינה גדולה בהרבה ובמקרים רבים האירוע מושתק. מספר המלצות שיעזרו לכם (ונקווה שלא תדרשו להן):

- **הדבר הראשון בעת התרחשות אירוע אבטחת מידע הוא לפעול בשיקול דעת** ? המלצה נכונה לכל מקרה שהוא. בשיקול דעת אני מכוון לפעולות שהיית מבצע לו היית צריך להיערך שלא בלחץ זמן/הנהלה/לקוחות. חשוב שלא לבצע פעולות מהן לא ניתן לחזור לאחור או שהן בעלות השלכות עסקיות בעיתיות.

- **נתחו את האירוע**. אספו במהירות כל מידע ותיעוד כדי שניתן יהיה לנתח את האירוע ולהבין מהו הנזק שנגרם וכיצד התרחש האירוע. ניתוח האירוע בהתבסס על נתונים כגון לוגים שמייצרות המערכות יאפשר הבנת הנזק, אופן התרחשותו והשפעתו.

- **בצעו פעולות מתקנות מיידיות**. נסו לצמצם את הנזק תוך אפשור פעילות עסקית תקינה ככל הניתן. מרגע שהבנתם כיצד התרחש האירוע נסו לבודד את מתחם הנזק, מנעו מהתחום הפגום להמשיך ולפגום בשאר הארגון. עדכנו את כל הגורמים שנדרשים לדעת אודות המקרה בהתאם לאירוע כגון לקוחות, הנהלה, דירקטוריון, גורמי פיקוח ובקרה (המפקח על הבנקים, המפח על הביטוח) וכו'.

- **אל תבצעו שינויים מערכתיים** (במערכות הפעלה, בסיסי נתונים, רכיבי תקשורת או אפליקציות) מבלי לבדוק שהמערכות מסוגלות להתמודד עם השינוי המוצע. ביצוע שינויים למערכות ייצוריות מבלי לוודא כי המערכת יכולה "לספוג" את השינוי עלולה להביא אתכם למצב ממנו יהיה קשה מאוד לחזור לאחור. המלצה פשוטה ? בדקו קודם על סביבת הניסוי או אים לא קיימת כזו פעלו בשלבים, כך שניתן יהיה לבודד כל שינוי ולחזור לאחור במידת הצורך.

- **התייעצו.** אין חכם כבעל ניסיון. נסו לקבל מה שיותר מידע באשר לפעולות שיש לנקוט. התיעצו עם עמיתים בארגון על מנת להבין השלכות עסקיות, התייעצו עם ארגונים דומים על מנת להבין כיצד הם פעלו, התייעצו עם יועצי אבטחת מידע מומחים.

- **אל תמהרו לרכוש מוצרי אבטחת מידע** מייד לאחר התרחשות אירוע בארגון. מטבע הדברים מעת לעת נפגע ארגון זה או אחר, בין אם מאירוע אבטחת מידע פנימי או מאירוע אבטחת מידע חיצוני. בשני האירועים נדרשים מנהל אבטחת המידע, מנהל מערכות מידע וגורמים נוספים להסביר בפני ההנהלה מהן הפעולות שנקטו על מנת שהאירוע לא יישנה. כדי למלא מענה זה בתוכן, נוטים פעמים רבות מנהלי אבטחת מידע לבצע רכש מהיר של מוצרי אבטחת מידע כדי מחד לטפל בבעיה הבוערת על הפרק ומאידך למלא את המענה להנהלה בתוכן. רכש זה, במקרים רבים אינו יעיל, אינו מותאם לארגון ואינו חלק מתוכנית אב לאבטחת מידע כי אם טלאי אבטחתי. ככזה פעמים רבות הוא יהפוך לנטל על הארגון ועל מנהל אבטחת המידע ברמת הניהול השוטף ולא בהכרח יספק מענה מתאים לבעיה המיידית.

- **אל תסתירו.** עדכנו את הלקוחות במידת הצורך. במקרים רבים לא ניתן להסוות את עצם התרחשות האירוע כמו במקרים של התקפות Phising . בהתקפות אלה נשלחים אלפי מיילים ללקוחות ולכאלה שאינם לקוחות במטרה "לדוג" לקוח אשר יסכים למסור פרטיו האישיים ולגנוב מחשבונו. התעלמות או הסתרת אירועים שייתכן בהחלט ויודעו לציבור הרחב יוצרת חוסר אמון בארגון שקשה מאוד לשקם. הודעה פשוטה ללקוחות אודות האירוע והפעולות הננקטות משתיקות את המקטרגים ומקנה ללקוח בטחון כי הוא מטופל.

- **בכל החלטה שתקבלו חשבו האם היא יישומית ברמת שגרת הארגון**. האם ניתן לממשה לאורך זמן והאם נדרשים משאבים קבועים לאחזקתה. ברבים מהמקרים הפתרונות טובים לטווח זמן קצר אולם לא ניתנים למימוש לאורך זמן ולכן אינם יעילים.

- **עשו כל שנדרש למניעת הישנות המקרה**. בפעם הראשונה זה לא נעים, בפעם השניה זו כבר הזנחה. פעלו על מנת להיות מוכנים הן ברמה הטכנולוגית והן ברמת הנהלים והתהליכים. בשום מקרה אל תשאירו את האירוע ללא טיפול מתוך תקווה שלא יישנה. בצעו רכש מתאים אשר ימנע את הישנות האירוע וישתלב בתפיסת אבטחת המידע של הארגון. נתחו תהליכים ארגוניים הדורשים רענון או המצריכים שינוי מלא, תעדו אותם בנוהל מחייב והפיצו אותו בקרב המעורבים. הכינו תוכנית מגירה לאירועים העשויים להתרחש (כנהוג בגופים בטחוניים) על מנת להגיע מוכנים לאירוע. "תרגלו" במידת האפשר אירועי דמי כגון התקפה על אתר האינטרנט, תקיפת וירוס ועוד. זכרו שפגיעה במערכות המידע בארגון תביא ברוב במקרים לפגיעה מיידית בעסקי החברה, ככזו אתם עומדים בקו הראשון של ההמשכיות העסקית.

כמו בכל תחום, גם בתחום ה - IT הגנב חוזר למקום הפשע. אל תבנו על כך ש"בזה הסיפור נגמר", בדרך כלל בזה הסיפור רק מתחיל.

הכותב הוא אורן שני,מנכ"ל אבנת אבטחת מערכות מידע וניהול סיכונים
http://www.avnet.co.il
oren@avnet.co.il

מקור המאמר: www.Articles.co.il - מאמרים לשימוש חופשי