

"אבטחת המידע הקלאסית פשטה את הרגל וקרסה"

"אנחנו מלמדים כל מנהל אבטחת מידע ארגוני להגן בחירוף נפש על אמינות, סודיות וזמינות", אמר איציק כוכב, הממונה על הגנת מידע בשירותי בריאות כללית ♦ לדבריו, "הדגש הדרמטי הוא על הצפנה של כל מידע שעומד או זז ברשת. אפשר להתחיל בהצפנת מידע הרגיש ביותר, ולאחר מכן - לעלות בדרגת החלת ההצפנה" ♦ "אנחנו צריכים לשנות את אחריות אבטחת המידע ולשנות את תפישת היישום"

יוסי הטוני

מידע אמיתי, הצורך באחסון, ירידה מסוימת בביצועים ופגיעה בממשק המשתמש. הגורם השלישי הוא שמנהלי מערכות מידע משדרים להנהלות שלהם ש'לי לא יקרה כלום בנושא אבטחת מידע' - ומבחינת עלות תועלת כדאי שלא להשקיע בפיתוח מאובטח. הגורם הרביעי קשור לתהליך ה-QA, במסגרתו לא בודקים שילוב וביצועי אבטחת מידע, בעיקר מסיבות תקציביות.

"לגבי המידע - המידע, מלבד זה הקיים בארגוני ביטחון, הוא מידע גלוי לא מוצפן, ולכן כל מי שהגיע אליו - איש המיחשוב, משתמש לא מורשה, נוכלי מידע - הגיע למידע אמיתי. עד לפני שנים היה חשש מלהצפין מידע, שכן ההצפנה גרמה לירידה בביצועים וההתעסקות עם החלפת המפתחות העיקה. יתירה מכך, בגלל העדר טכנולוגיה בשלה

ותרבות המנהלים, אין בקרה הדוקה על המשתמש. כיום כמעט ולא ניתן לדעת מי צפה במידע, מי ערך את המידע, מי הדפיס את המידע, מי שלח את המידע, מי הוציא את המידע להתקן חיצוני. ובוודאי שלא ניתן לדעת מי ממנהלי המערכת ואנשי המיחשוב עשה, ומה עשה במידע".

אתה מציג מצב מביך שבו המידע למעשה אינו מוגן בכל נתיבו. אז מה הפתרון?

"אנחנו צריכים לשנות את אחריות אבטחת המידע ולשנות את תפישת היישום. לפי דעתי, אחריות אבטחת המידע היא אמינות המידע, סודיות המידע ובקרה על המידע. אלו ייושמו באמצעות 'מודל הכוכב', שבו המידע מצוי במרכז הכוכב וכל פאה מייצגת פעולה על המידע. על המידע תבוצע הצפנה. המידע ייעטף במדיניות, והגישה למידע תבוצע באופן חד משמעי ועל המידע תבוצע בקרה".

פרט יותר את "מודל הכוכב".

"תקציב אבטחת המידע שיוקצה, יאפשר יישום של המודל במלואו, בעוד היום הוא מנוצל ברובו על זמינות המידע. לגבי הצפנת המידע - עולם הצפנת המידע בשל כמעט ואין ירידה בביצועים בשל עריכת הצפנה. ניהול המפתחות קל ליישום והרעיון הוא שכל מידע אמיתי יוצפן כבר בשלב יצירתו. אין צורך להצפין את כל המידע שבבסיס הנתונים: אפשר להצפין רק את החלק הרגיש והנפיץ של המידע. גם את התקשורת יש להצפין לכל אורכה, וזאת כדי שאם פרצו אליה -



איציק כוכב

הזמנים השתנו: אבטחת המידע הקלאסית, שלאורה גדלנו ואותה מימשנו שנים רבות, פשטה את הרגל וקרסה", כך אמר **איציק כוכב**, ממונה הגנת מידע בשירותי בריאות כללית.

כוכב התראיין לאנשים ומחשבים בעקבות דבריו במפגש פורום CISO, מנהלי אבטחת מידע של אנשים ומחשבים. לדבריו, "אנחנו, אנשי אבטחת המידע, שגינו בתפישת האבטחה". כוכב הוא בעל קילומטראז' של 40 שנים באבטחת מידע בארגוני ביטחון ובריאות.

ההכרזה הזאת קצת קיצונית, הלא כן ?

"ראה מה קרה בעולם ובישראל בשנים האחרונות. פרשות ענת קם, אדוארד סנואודן, ויקיליקס, אנונימוס, ארגוני האקרים ממדינות עוינות ועוכרי ישראל. ואצלנו, המשתמש די

שוב ואינו ממושמע - ומנהלי מערכת ניגשים ויכולים לראות כל מידע. "כולם הצליחו להגיע למידע ובחלק מהמקרים איש לא גילה שעשו כך. אני קובע שאפשר להגיע לכל מידע שרוצים. זה רק עניין של זמן, כוח מיחשוב ותחכום אנושי. והצער שבדבר הוא, שכאשר מגיעים למידע, מתברר כי הוא גלוי ולא מוצפן".

למה זה קרה ואיפה כשלתם ?

"אבטחת המידע הקלאסית, תפקידה לשמור על אמינות המידע, זמינות המידע וחיסיון המידע. תפקיד זה מבוצע באמצעות מודלים להגנה, שהפופולרי ביניהם הוא מודל שבע השכבות בסדר היורד הבא: מדיניות, הגנה פיזית, הגנה על התקשורת החיצונית, הגנה על התקשורת הפנימית, הגנה על תחנת המשתמש, הגנה בפיתוח והגנה על המידע עצמו".

בפועל, תקציבי אבטחת המידע מנוצלים על ארבע השכבות הראשונות. מדוע נוצר מצב זה? מדוע אינכם מגיעים ליישום השכבות העמוקות?

"לגבי המשתמש - הרי שהמשתמש מפונק, מנהל מערכות המידע לא מעוניין להכביד עליו עם דרישות אבטחת מידע. המנמ"ר רוצה להיות שירותי..."

"לגבי שילוב אבטחת המידע בפיתוח - כאן יש כמה גורמים משפיעים. הראשון, שכל תוספת של דרישות אבטחת מידע מאריכה את שלב הפיתוח. השני הוא שדרישות אבטחת מידע הן יקרות: הקמת סביבות ללא