לא יגיעו למידע גלוי. וכך גם יש להצפין את ההתקנים החיצוניים. פתרון זה יגרום לכך שהמידע לכל אורך נתיבו יהיה מוגן.

"לגבי מימוש מדיניות אבטחת מידע על המידע עצמו: כל קובץ בכל צורה 'ייעטף' בשכבת מדיניות. על פי המדיניות ייקבע למי מותר לראות את המידע, מה מותר למשתמש לעשות עם המידע - צפייה או עריכה, לאן מותר לשלוח את המידע, מי יקבל התראה שנגעו במידע, כמה זמן המידע יהיה נגיש למשתמש. פתרונות אלה כבר קיימים בשוק מזה כמה שנים - והם בשלים.

נתיב המידע

"אני נוהג להשתמש במונח 'נתיב המידע'. נתיב המידע הוא כל אורך הדרך שמידע רגיש נחשף לאדם. בכל תחנה שכזו לאורך נתיב המידע דרושה מדיניות אבטחת מידע: המשתמש, עובר אורח תמים, איש מיחשוב ותקשורת, ספק חיצוני, נוכל מידע, האקר".

ומה לגבי הזדהות חד משמעית?

"הכוונה היא לגרום למצב שכל מי שניגש למידע, אכן הוא זה שהורשה לגשת למידע. כדי להדק את האכיפה הזו ולמנוע מניפולציות, אני ממליץ על זיהוי ביומטרי של טביעת אצבע וקוד בן ארבע ספרות באמצעות כרטיס MOC - ולא הקמת מאגר ביומטרי. בעתיד הלא רחוק נשתמש בהזדהות שכזו.

"לגבי בקרה על המידע, מחקרים וגם חיי היומיום של מנהלי אבטחת מידע, מוכיחים כי אם המשתמש יודע שיש עליו בקרה - הוא מתנהג עם המידע על פי הנהלים והאבטחה שנקבעו. הכוונה שייקבעו לכל מערכת חוקי אנומליה ואם המשתמש חצה אותם - תתקבל התראה במרכז התראות אבטחת מידע, SOC. הכוונה היא לאנומליות ברמת המערכת, ברמת תחנת המשתמש, ברמת מנהל המערכת ואיש מיחשוב ותקשורת וברמת הרשת.

"לגבי פיתוח מאובטח, יש לחייב כל מנהל פיתוח לפתח את היישום בקוד מאובטח, לייצר חוקי אנומליה, להקים תשתית למערך הרשאות למשתמשים ומערך הרשאות למנהלי המערכת. יש לאפשר ליישום יכולת דיווח של אירועי אבטחת מידע למרכז בקרת אירועי אבטחת מדע, SOC. יש לייצר log אל כל התרחשות במערכת - מי ניגש למידע, מתי ניגש למידע ומה עשה עם המידע.

"תהליך הפיתוח של מערכת, או אפיון תהליך או"שי (ראשי תיבות ארגון ושיטות) הם בבחינת 'תקופה פרועה' מבחינת אבטחת מידע. בשלב זה מוותרים על אבטחת מידע ומייצרים בכך תשתית לא מאובטחת - גם טכנולוגית וגם תרבותית. בשלב הפיתוח יש חובה להקים כמה סביבות תוך שימוש בנתוני דמה. כך גם בסביבת ה-QA, סביבת בדיקות, וסביבת ההדרכה. נתוני אמת יופיעו רק בייצור. מצב זה ימנע חשיפת מידע רגיש בשלבי הפיתוח ובעת בניית התהליך".

זמינות המידע - למנמ"ר

ומה עם סוגיית זמינות המידע?

"אני סבור שכל עולם זמינות המידע הוא חלק מאחריות ותפקיד מנהל מערכות המידע. זאת כי הוא צריך לספק מערכת עובדת, זמינה, ידידותית. זמינות אינה מתפקיד מנהל אבטחת המידע. ברור שהאתגר לספק זמינות מידע יושפע גם מדרישות אבטחת המידע ויוסיף לאתגר של מנהל מערכות המידע".

> "הכוונה היא לגרום למצב שכל מי שניגש למידע, אכן הוא זה שהורשה לגשת למידע. כדי להדק את האכיפה הזו ולמנוע מניפולציות, אני ממליץ על זיהוי ביומטרי של טביעת אצבע וקוד בן ארבע ספרות באמצעות כרטיס MOC - ולא הקמת מאגר ביומטרי"

ואתה חושב שכל זה אפשרי?

"אני משוכנע בכך לחלוטין. הרי במגזר הביטחוני זה כבר קורה. תקן PCI גרם לכל המשק לבצע הצפנה של נתוני כרטיסי אשראי כבר בשלב העברת הכרטיס במכונות הסליקה השונות. יש פתרונות טכנולוגיים לכל המודל והם בשלים. מנהל צריך להפנים שאם המידע יוצפן כבר בשלב יצירתו - הרי שאם זר יגיע למידע הוא יגיע למידע לא מובן. ובכך לא ייפגעו האדם והארגון. אולם את מודל הכוכב ניתן יהיה ליישם ולהטמיע כתפישה, רק

אם יבוצע תהליך של חינוך והכשרה בכל רמות החינוך: בתי ספר תיכון, מכללות, אקדמיה ובעיקר בתרבות הארגונית".

אתה טוען שאתם כמנהלי אבטחת המידע שגיתם בתפישת הפתרון. איפה טעיתם?

"אני חושב שעוצמת הצורך והמקום בניהול אבטחת מידע בצורה רחבה התפתחו משמעותית בשנים האחרונות. כנגזרת, ההכרה בצורך והנכונות להשקיע בנושא עלו משמעותית. תחום אבטחת המידע במגזר האזרחי חווה שינויים דרמטיים, שיילכו ויתעצמו בעתיד הקרוב. אחת התובנות המתהוות נעוצה במיקום של פונקציית אבטחת המידע בארגון. היא תעבור ממקום של פונקציה שממוקמת כחלק ממחלקת מערכות מידע ומעניקה בעיקר פתרונות טכנולוגיים - למקום שרואה את תמונת הארגון הכוללת, על כל רבדי תפישת אבטחת המידע.

"פונקציה זו, ראוי שתימצא ברמת הנהלת הארגון ותמלא גם את תפקיד ממונה פרטיות המידע. היום, 90% ממנהלי אבטחת המידע כפופים למנהל מערכות המידע. מכאן נובע הכשל ובשל כך שגינו - כי לא 'הרמנו את ראשנו' בזמן".