Zalmanovitsh David
Attorney at law, B.A, LL.B, M.B.A
CEO
www.glawbal.com

ניהול סיכונים, אבטחת מידע וניהול ידע בסביבת עבודה משפטית - נובמבר 2007

כנעשה בעולם מזה שנים רבות, גם בארץ גדלה המודעות וההערכות של משרדי עורכי דין ומחלקות משפטיות לנושאי ניהול הסיכונים, ניהול ידע ואבטחת מידע. סיכונים אלו רבים, שונים ומגוונים ולכך הקדשנו בעבר טורים שונים. לסיכונים אלו השקה לנושא אחריות מקצועית ואנו רואים יותר ויותר אירועים ותביעות אחריות מקצועית אשר עילתן כשלים בנושא ניהול ידע ואבטחת מידע.
לאחרונה ובין השאר בעקבות מקרה "הסוס הטרויאני" והשלכותיו, גם וועדת המחשוב של לשכת עורכי הדין נדרשה לנושא והפיקה מדריך לאבטחת מידע והגנה על הידע, כמו גם הקשר של הללו לכללי האתיקה והדין הכללי. מדריך זה ניתן לאיתור באתר האינטרנט של לשכת עורכי הדין.

לרגל יום עיון בינלאומי שנערך בחודש שעבר בנושא, בהשתתפותם של מרבית השותפים המנהלים של המשרדים הגדולים ומנהלי מחלקות המשפטיות ומרצים בתחום מהארץ ומחו"ל, בחרנו להקדיש מאמר קצר זה לנושא ניהול סיכונים ממערכות המחשב והידע שלנו ולסקירה קצרה של המדריך הנ"ל.
כמו כן ביקשנו ממנכ"ל חברת אבטחת המידע 2Bsecure המייעצת למשרדי עורכי דין ולמחלקות משפטיות בנושא אבטחת מידע, הייתה מעורבת בגילוי הסוס הטרויאני וסייעה ללשכת עורכי הדין בניסוח הכללים הנ"ל, ולהתייחס בשולי מאמר זה, לנושא גישה מרחוק למערכות הארגון.

מה אורב לנו ביום יום?
שאנו בוחנים את אירועי ניהול הסיכונים ואבטחת מידע בתחום מערכות המחשב וניהול הידע אנו מאפיינים מספר קבוצות מרכזיות:
חשיפה פיסית – בקבוצה זו נכללים כל האירועים בהם אנו נחשפים לפריצות או לשריפה או לגניבה של תכנים או חומרים השייכים למשרד או ללקוחותיו. כאן יימנו, לדוגמא, מקרים אמיתיים הכוללים גניבתו של שרת הקבצים ממשרד פלוני, נטילתם של תיקי לקוח ומחשב נייד ממכוניתו של שותף במשרד אחר או אירוע של הצפת מים בארכיב של משרד שלישי.
חשיפה אלקטרונית –כאן נמנים כל אותם עשרות מקרים ואירועים בהם נחשף הידע על המשרד ולקוחותיו לצדדים שלישיים באמצעות חדירה לחומר מחשב, הזנחה וטיפול שגוי בנושא ניהול ההרשאות והסיסמאות, העברה יזומה של חומר מהמשרד באמצעות דואר אלקטרוני, כשלים בגיבוי המידע הקיים במשרד – עד כדי אובדן ידע על לקוחות, אותו לא ניתן לשחזר, כשלים בהתחברות עובדי המשרד מחוץ למשרד, אובדן של תקליטורים ובהם קבצי מידע המורדים מרשת המחשב של המשרד וכדומה.

חשיפה בניהול הידע - בעבר הקדשנו טור שלם לנושא ניהול הידע במשרד עורכי דין וחילקנו אותו למספר קבוצות: מהמידע הכללי העוסק בנושאים כגון מידע על התנהלות בסביבת העבודה ונהלים, דרך ידע ציבורי העוסק בדוגמאות חוזים וטפסים מזה וחידושי פסיקה וחקיקה מזה ועד הידע הצבור לנו על לקוחותינו הן באופן פיסי והן באופן אלקטרוני. נקודות החשיפה בקבוצה זו רבות מאוד, מחשיפת המשרד לפגיעה במוניטין שלו וניהול הזמן שלו עת הינו לדוגמא משתמש בהסכמים ובטפסים שונים לאותו סוג של עסקאות, דרך חוסר עדכון עובדיו בחידושי פסיקה וחקיקה ועד חוסר סדר וארגון כמו גם אובדן של חומר עובדתי ומשפטי, בתיקי לקוחות.

בכל אחת מן הקבוצות יש כדי לחשוף אותנו לאובדן זמן, אובדן כסף, פגיעה במוניטין ובמקרים קיצוניים גם תביעות אחריות מקצועית.

אין לעשות שימוש להפיץ ו/או לשכפל ו/או לצלם מסמך זה ו/או חלקו ללא אישור

אין לראות באמור במסמך זה כייעוץ ו/או חוות דעת מקצועית כלשהי

העושה שימוש באמור במסמך זה ותוכנו עושה זאת על אחריותו בלבד

GLawBAL
Enhancing Performance

Zalmanovitsh David
Attorney at law, B.A, LL.B, M.B.A
CEO
www.glawbal.com

כיצד נגן על עצמנו?
על קצה המזלג ננסה לסקור את סוגי ודרכי ההגנה הקיימות לנו אל מול 3 קבוצות הסיכונים שמנינו:
ההגנות הפיסיות - הקיימות לנו נעות מבקרה נכונה של סביבת העבודה וניטור הכניסות אליה, טיפול בארכיב הפיסי או חדר המחשבים מפני הצפה או אש ועד כללים ונהלים ברורים העוסקים בנושא הוצאת חומר מן המשרד, ניודו של חומר ברכב, שמירתו של חומר בבית העובדים, גריסתו של חומר רגיש וכיוצא באלו.
ההגנות האלקטרוניות - הינן רבות ומגוונות: ראשיתן בכללי עבודה ברורים ואחידים לשימוש במערכות המחשב, להרשאות של משתמשים, לגיבוי החומר האגור בנוהל מסודר והוצאתו מהמשרד, למיפוי ותיעוד המערכות הטכנולוגיות של המשרד, לשימוש נכון בדואר האלקטרוני ורשת האינטרנט ועוד כללים ונהלים חשובים. גם הטכנולוגיה באה לעזרתנו במשפחת הגנות אלו ויצרה כלי הגנה שונים כגון: "חומות אש" לגישה מבחוץ למערכות המשרד, תוכנות מעקב תיעוד וניהול לוגים, הגנות וירוסים ועוד כלי תוכנה וכללים הנלווים להם, אשר יתנו בידינו: הן הגנה מונעת והן הגנה וטיפול מקום בו נחשפנו או נפגעו מערכות המחשב והידע שלנו.
הגנות בניהול ידע – הללו תעסוקנה בריכוז וניהול הידע לסוגיו השונים באמצעות נהלים וכלים טכנולוגיים לניהול מסמכים וידע. כך נארגן את הידע הציבורי לגווניו בתיקיות ציבוריות בשרת הקבצים או שרת הדואר עם גישה קלה למשתמשי המשרד. כך נשקול האם לרכוש תוכנות ייעודיות לניהול מסמכים וידע מכל סוג ובפרט על לקוחות ובהשקעה קטנה, ננהל את הידע באופן מאורגן, זמין, יעיל ובטוח. כך גם ניזום ונקפיד על מספר כללי עבודה בסיסיים כגון: ניהול גרסאות הסכמים או מסמכי בית דין, ניהול נכון ומסודר של הארכיב הפנימי והחיצוני, ניהול ותיוק מסודר של ההתנהלות האלקטרונית מול הלקוח וכיוצא באלו.

ניהול ידע ואבטחת מידע – דין ואתיקה
מהי חובתו של עורך דין מהדין והאתיקה בנושאי אבטחת הידע? האם זו שאלת "קיטבג" או שאלה ראויה המקימה לעורך הדין חובות מהדין הכללי וחובות אשר עניינם גם אתיקה מקצועית.
בשנת 2004 ועל רקע אירועי הסוס הטרויאני אשר הוחדר גם למשרדי עורכי דין, החליטה וועדת המחשוב של לשכת עורכי הדין, לנפק מדריך לנושאי אבטחת מידע לעורכי דין. המדריך אינו מתיימר לקבוע כי אי קיום הוראותיו מהווה ראיה להפרת הדין או כללי האתיקה, אך יחד עם זאת קובע מספר דברים ובין השאר כי:

- על פי כללי האתיקה עורך הדין חייב לנקוט אמצעים סבירים כדי לשמור על פרטיות הלקוח ועל סודיות המידע שהועבר בינו לבין הלקוח.
- חובת הסודיות אינה תלוית טכנולוגיה ועל עורכי הדין חלה חובה אתית לנקוט אמצעים לאבטחת המידע המצוי במערכות המחשב שברשותם.
- ייתכן ועורכי דין שאינם נוקטים אמצעים סבירים לאבטח את מערכות המחשב שלהם וכתוצאה מכך הועבר מידע לצדדים שלישיים, ימצאו מפרים את חובת הסודיות הקבועה בסעיף 19 לכללי לשכת עורכי הדין (אתיקה מקצועית), התשמ"ו – 1986 ובנוסף הם עלולים לחוב באחריות אזרחית, בין היתר מחמת רשלנות או בגין הפרת חוק הגנת הפרטיות.

גישה מרחוק למערכות המשרד (מאת מר אלון מנצור מנכ"ל חברת 2BSecure)
במשרדי עורכי דין כמו גם במחלקות משפטיות נדרשים העובדים מעת לעת להתחבר למערכות הארגון מרחוק. לאחרונה הצורך בחיבור מרחוק למערכות המשרד הפך לנפוץ הרבה יותר מבעבר: אם בשעות לילה מהבית, בעת נסיעות לחו"ל, שיחות ועידה וכד'. ניסיוננו מלמד כי במקרים רבים גישה זו למערכות המשרד נעשית עדיין באופן מסורבל המקשה על המשתמש ובמקרים רבים חושף אותו ואת הארגון לכשלי אבטחת מידע רבים.

אין לעשות שימוש להפיץ ו/או לשכפל ו/או לצלם מסמך זה ו/או חלקו ללא אישור

אין לראות באמור במסמך זה כייעוץ ו/או חוות דעת מקצועית כלשהי

העושה שימוש באמור במסמך זה ותוכנו עושה זאת על אחריותו בלבד

Zalmanovitsh David
Attorney at law, B.A, LL.B, M.B.A
CEO
www.glawbal.com

מעטים יודעים כי בהקפדה על מספר כללי עבודה פשוטים והטמעת מערכות שעלותן קטנה ניתן הן לשפר את זמינות ואיכות הגישה מרחוק למערכות המשרד והן את רמת אבטחת המידע.
נמנה להלן מספר עקרונות וכללים אשר מערכות מתקדמות מאפשרות בעת גישה של משתמשי קצה למערכות הארגון:
הצפנה – מערכות מתקדמות יוצרות די בפשטות, גישה מרחוק למערכות המשרד באמצעות תקשורת מוצפנת על ידי ביסוס רשת פרטית וירטואלית (VPN) ותקני הצפנה המקובלים גם באתרי קניות ובבנקים.
רשת הגנה – על הגישה לרשת הארגון להיות מותנית בעמידה בסטנדרטים מקובלים של הגנה מפני וירוסים באמצעות תוכנות הגנה מקובלות. לדוגמא, מערכות מתקדמות מזהות את המחשב ממנו נעשית הגישה מרחוק וסוקרות את רמת האבטחה שלו.
הזדהות – כיום אין יותר צורך בזיהוי ארוך ומתיש והטכנולוגיה העדכנית מאפשרת זיהוי פשוט ומאובטח מכל מחשב קצה בבית, בשדה התעופה ואף מאינטרנט קפה.
הרשאות – גם בנקודה זו נעשתה כברת דרך רבה ובמערכות מתקדמות נקבעת רמת הרשאות הקובעת לאיזה מיישומי הרשת הארגונית יהיה רשאי העובד לגשת מרחוק.

עו"ד זלמנוביץ דודי מנהלה של חברת GLawBAL המתמחה בהשמה ובייעוץ ובשיפור ביצועים של משרדי עורכי דין. אין להסתמך על הכתוב כייעוץ או כחוות דעת מקצועית.

אין לעשות שימוש להפיץ ו/או לשכפל ו/או לצלם מסמך זה ו/או חלקו ללא אישור

אין לראות באמור במסמך זה כייעוץ ו/או חוות דעת מקצועית כלשהי

העושה שימוש באמור במסמך זה ותוכנו עושה זאת על אחריותו בלבד