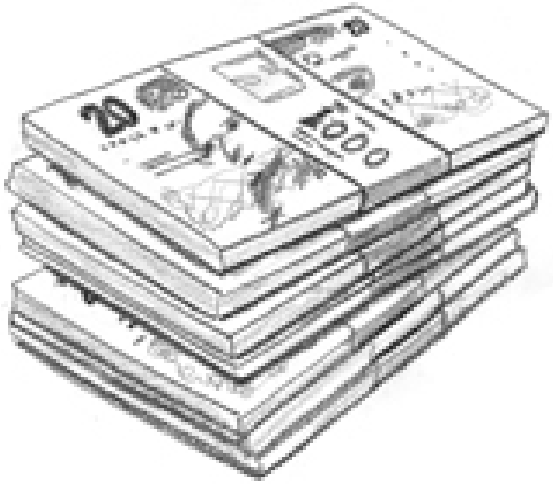
Fahn Kanne
Grant Thornton

סקרי סיכונים במערכות מידע בצל המשבר כלכלי



רמי ניסן

מרץ 2009

Fahn Kanne Control Manegment Ltd. All rights reserved.

"האמת הייתה יכולה להיות הרבה יותר פופולארית, אילולא חשפה תמיד עובדות מכוערות".

הנרי האסקינס

Fahn Kanne Control Manegment Ltd. All rights reserved.

על מה נדבר...

- בואו נעשה סדר - מה זה בכלל?
- באילו תחומים מתמקד סקר סיכונים במערכות המידע.
- סקרי סיכונים בצל המשבר.

Fahn Kanne Control Manegment Ltd. All rights reserved.

מן הכותרות

עובד ממורמר השתלט על רשת המחשבים העירונית של סן פרנסיסקו

באמצעות יצירת סיסמה שנתנה לו גישה וחסמה אותה עבור משתמשים אחרים, השיג העובד גישה בלתי מוגבלת למאגרי המידע של העירייה שהכילו תכתובות אימייל של העובדים, נתוני שכר, מסמכים מסווגים של רשויות החוק ומידע על אסירים

AP וכלכליסט – 17.7.08

4,000 שרתים ניצלו ממתקפה של עובד ממורמר

כ-4,000 מהשרתים של פאני מיי ניצלו ממתקפה שאיימה להרוס את כל המידע שבהם רק בזכות ערנותו של אחד מעובדיה. מה בדיוק קרה שם ואיך תוכלו לצמצם את הסיכוי למתקפה כזו גם בארגון שלכם?

עובד ממורמר שפוטר מחברת פאני מיי, אחד מהתאגידים הגדולים בארצות הברית בתחום המשכנתאות, הטמין במערכת המחשבים של החברה קוד זדוני שאמור היה להרוס את המידע בכל ארבעת אלפי השרתים שלה ולגרום לנזק הנאמד במיליוני דולרים. רק בזכות ערנותו של אחד העובדים האחרים בחברה סוכלה המזימה בזמן. אתר "תפוז"

מאת: עורב צפוני 02/02/09 13:53

וירוס שהחדיר עובד היי-טק ממורמר שיבש מערכות בבנק לאומי

הודה כי החדיר וירוס למערכת המיחשוב של בנק לאומי, לאחר שפוטר מחברת ההיי-טק דרכה הועסק כקבלן

Globes - 17/10/07 15:10

הערכת הסיכונים במערכות מידע

- **סיכון** - האפשרות שאיום כלשהו ינצל פגיעות (חשיפה) של נכס (או יותר), ויגרום עקב כך להפסד, או לנזק לנכסי הארגון.
- **נכסים לדוגמא**: נכסי מידע וידע, חומרה, תוכנה, שירותים שהארגון נותן, מוניטין, עובדים, רכוש וכד'.
- **איומים לדוגמא**: שגיאה (בתום לב), הונאה, מעילה, אסון טבע, פגיעה במכוון (מבפנים או מבחוץ), כשל מערכות וכד'.
- **חשיפות לדוגמא**: חוסר ידע, אבטחת מידע לקויה, עובד ממורמר, היעדר אבטחה פיזית וכד'.

Fahn Kanne Control Manegment Ltd. All rights reserved.

מהו סקר סיכונים

- כלי לאיתור מוקדי סיכון בתחום ב- IT של הארגון.
- מטרת ניתוח סיכונים הינה לאתר תהליכים ונושאים אשר חשופים בצורה מוגברת לסיכונים.
- ככל שתהליך או נושא מסוים חשוף יותר לסיכונים, על הנהלת החברה להפנות משאבים ניהוליים לפעולות תכנון ובקרה מתאימות.
- סקר הסיכונים מאפשר לחברה להתמקד באותם תחומים, אשר להם חשיפת יתר לסיכונים.

Fahn Kanne Control Manegment Ltd. All rights reserved.

מתודולוגיה לביצוע סקרי סיכונים

- זיהוי הנכסים הנדרשים להגנה.
- זיהוי האיומים הקיימים על נכסים אלו.
- הערכת ההשפעה או הנזק שייגרם במידה והאיום יתממש.
- הערכת ההסתברות למימוש האיום.
- הערכת הסיכון: הנזק הפוטנציאלי * ההסתברות למימוש.

– סיכון כולל (Overall): הערכת הסיכון ללא התחשבות בבקרות הקיימות.
– סיכון שאריתי (Residue): הערכת הסיכון הנותר, בהתחשב בבקרות הקיימות.

Fahn Kanne Control Manegment Ltd. All rights reserved.

שיטת ניתוח הסיכונים

שיטת ניתוח הסיכונים

לגבי כל תהליך ונושא תוגדר רשימה של סיכונים פוטנציאלים. לגבי כל סיכון ייבחנו שני פרמטרים: עוצמה והסתברות להתרחשויות.

קביעת עוצמת הסיכון

עוצמת הסיכון מוגדרת לפי שלושה פרמטרים:

- הנזק הכספי העלול לנבוע מהתממשות הסיכון.
- חשיפה משפטית.
- חשיפה לפגיעה במוניטין או בגורמים אחרים.

כל אחד מהסיכונים ידורג בציון של 1-5 המאפיין את רמת הנזק הפוטנציאלי שיגרם לארגון במקרה של התממשות הסיכון.

Fahn Kanne Control Manegment Ltd. All rights reserved.

שיטת ניתוח הסיכונים

2. קביעת ההסתברות להתרחשות הסיכון

ההסתברות להתרחשות הסיכון מחושבת בהתאם למאפייני הסיכון שהוגדרו.

להלן רשימת מאפיינים פוטנציאליים לסיכון:

- מורכבות המערכת (אפליקציה, רשת, מתקן וכד')
- קיום נהלים
- חשיפה למעילות
- מוטת שליטה (מבנה ארגוני, רשתות תקשורת, מתקני מחשוב)
- שינוי משנים קודמות (מערכות חדשות, רשתות חדשות, הסבות וכד')
- בדיקות שבוצעו בשנים האחרונות: ביקורת אבטחת מידע, בדיקת חדירות וכד'
- הערכת ההנהלה

כל אחד ממרכיבי הסיכון ידורג בציון של 1 עד 5, כאשר 1 משקף רמת סיכון נמוכה ו-5 משקף רמת סיכון גבוהה.

Fahn Kanne Control Manegment Ltd. All rights reserved.

חישוב העוצמה

נושא/ יחידה ארגונית	תיאור הסיכון	עוצמה				סה"כ עוצמה
		כספי	חשיפה משפטית	מוניטין / אחר		
		משקל				
		5	2	3		
		ציון	ציון	ציון		
Y	א	3	3	5		3.6
	ב	5	4	5		4.8
	ג	4	3	5		4.1
	ד	4	5	1		3.3
	ממוצע					4.0
Z	ה	3	5	1		4
	ו	2	2	1		4
	ז	3	1	1		5
	ממוצע					4.3

Fahn Kanne Control Manegment Ltd. All rights reserved.

חישוב ההסתברות

נושא/ יחידה ארגונית	תיאור הסיכון	הסתברות								סה"כ הסתברות
		מורכבות המערכת	קיום נהלים	חשיפה למעילות	מוטת שליטה	חשיפה משפטית	שינוי משנים קודמות	בדיקות בשנים האחרונות	הערכת ההנהלה	
		משקל								
		5	2	5	4	3	2	2	2	
		ציון	ציון	ציון	ציון	ציון	ציון	ציון	ציון	
Y	א	4	5	5	1	4	1	5	1	3.40
	ב	4	5	5	5	4	3	5	5	4.52
	ג	4	4	5	3	4	1	5	4	3.88
	ד	4	4	1	1	2	2	5	1	2.36
	ממוצע									3.5
Z	ה	3	5	1	1	2	1	5	1	2.16
	ו	2	2	1	2	4	1	5	2	2.20
	ז	3	1	1	2	5	1	5	1	2.36
	ממוצע									2.24

עמוד 1

Fahn Kanne Control Manegment Ltd. All rights reserved.

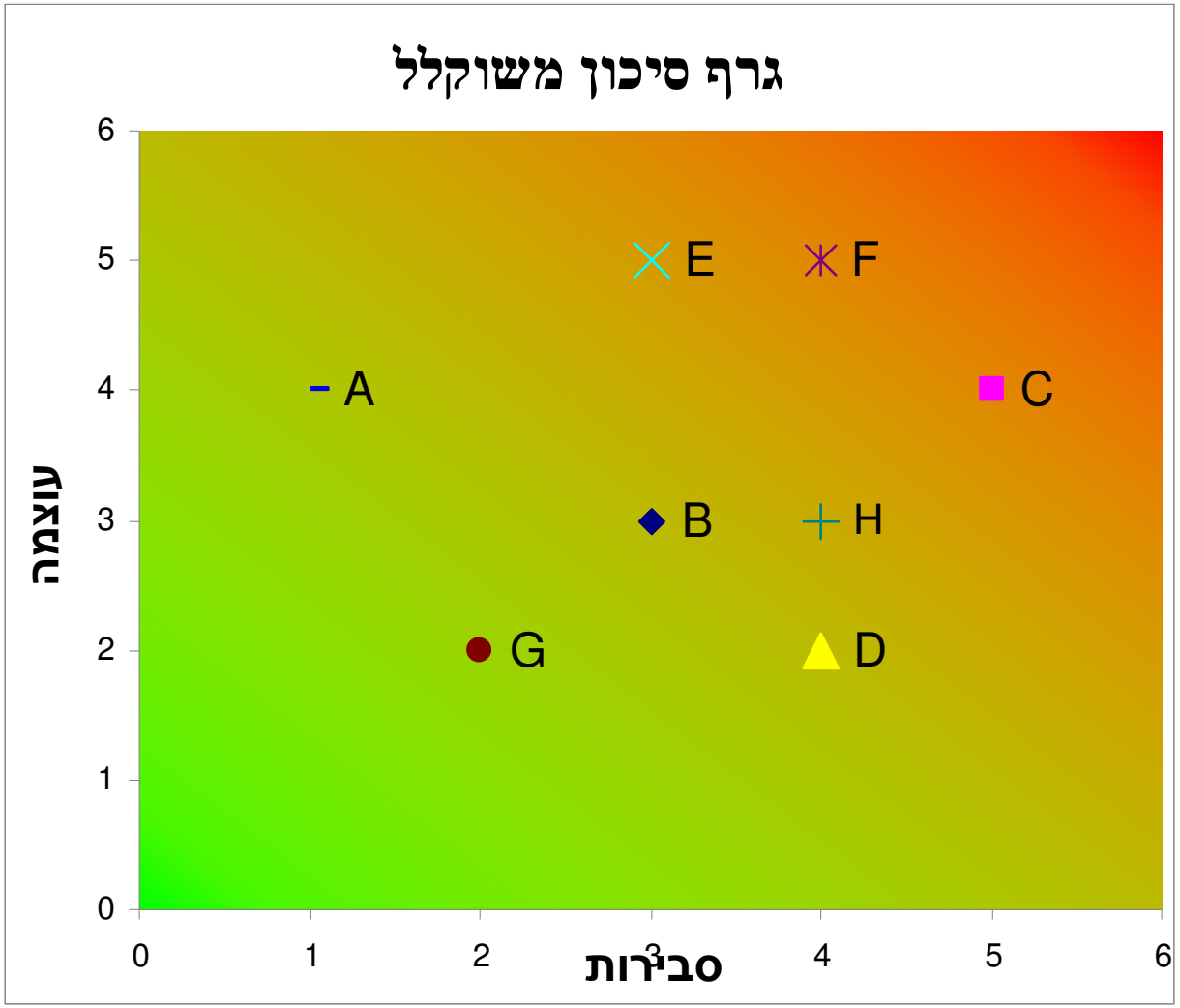
חישוב רמת הסיכון המשוכללת

נושא/ יחידה ארגונית	תיאור הסיכון	עוצמה	הסתברות	רמת חשיפה			
		סה"כ עוצמה	סה"כ הסתברות	עוצמה X הסתברות		חשיפה לתהליך	ציון לתהליך
Y	א	3.6	3.40	C	12.24	14.41	C
	ב	4.8	4.52	A	21.70		
	ג	4.1	3.88	B	15.91		
	ד	3.3	2.36	D	7.79		
	ממוצע	4.0	3.5				
Z	ה	4	2.16	D	8.64	9.75	D
	ו	4	2.20	D	8.80		
	ז	5	2.36	C	11.80		
	ממוצע	4.3	2.24				

עמוד 1

Fahn Kanne Control Manegment Ltd. All rights reserved.

גרף סיכון משוכלל



התחומים העיקריים להתייחסות במסגרת סקר הסיכונים

- ניהול שינויים במערכות המידע.
- פיתוח מערכות.
- אבטחת מידע.
- תפעול מחשוב.

Fahn Kanne Control Manegment Ltd. All rights reserved.

חשיבות ביצוע סקר סיכונים בתקופת המשבר

- המשבר הכלכלי עלול להוביל חברות למאמץ גדול יותר ליצירת קיצורי דרך יצירתיים. ביניהם, ריגול תעשייתי, בדגש על ניסיונות להשיג מידע ממערכות המידע של חברות מתחרות או של לקוחות. כמו כן, צפויים ניסיונות לקבל או לקנות מידע מעובדים שפוטרו.
- השקעה בניהול סיכונים אינה נותנת תמורה בעין, ולכן חברות בקשיים נוטות לצמצם את השקעותיהן בניהול הסיכונים בכלל, ובתחום מערכות המידע בפרט. דבר זה מוביל לחשיפה מוגברת של הארגון לסיכונים.
- קיצוץ בכ"א.
  - תחזוקה לקויה של המערכות.
  - חוסר בבקרה כתוצאה מויתור על הפרדת תפקידים ראויה.

Fahn Kanne Control Manegment Ltd. All rights reserved.

חשיבות ביצוע סקר סיכונים בתקופת המשבר - המשך

- המש
  עובד
  - לשא
  - לפג
  - למר
  - ועוד
- שימו
  לתב
- הפח

ת בעבודה.

ארגונים

ר יציבות

ברשת.

הצד האפל של ה-IT

מתכנת לשעבר במשרד התמ"ת נאשם במכירת מידע לבעלי עניין

בכתב האישום שהוגש אתמול (ב') נטען, כי איש המחשבים העביר בעת עבודתו במשרד, מידע על אנשים שהגישו בקשות להעסקת עובדים זרים לידי קבלן כוח אדם באשקלון - עובדה שאפשרה לבעל המשרד לפנות אל מגישי הבקשה ולהציע להם עובדים לפני המתחרים שלו • בין סעיפי האישום: לקיחת שוחד, מרמה והפרת אמונים, הפרת חובת סודיות בשימוש במאגרי מידע, שימוש שלא כדין במאגר מידע וחדירה לחומר מחשב כדי לעבור עבירה אחרת

יהודה קונפורטס, מערכת DailyMaily, ThePeople

05/08/2008

Fahn Kanne Control Manegment Ltd. All rights reserved.

חשיבות ביצוע סקר סיכונים בתקופת המשבר - המשך

- חיסכון באמצעי מיגון ומערכות אבטחה, מגביר את החשיפה הקיימת למערכות ולמידע בארגון.
- צמצום בפעילות הביקורת והבקרה השוטפת (הן בתדירות והן בכמות) יחשוף את הארגון לטעויות, מעילות ועוד.

ts reserved.

המסקנה

1. אל תחכו לרגולציה... דווקא עכשיו מומלץ כי היוזמה לסקר הסיכונים בתחום ה- IT תבוא מהמנמ"ר. היא עשויה להתגלות כמשתלמת...
2. יש להתאים את הנושאים והתחומים הנבחנים בסקר למציאות החדשה.
3. גם אם בוצע בשנה האחרונה סקר סיכונים, וזוהו כל הסיכונים באופן ראוי, רצוי לבחון שוב את הניתוח שבוצע לכל אחד מהסיכונים, שכן ייתכן שהסבירויות והעוצמות שהיוו בסיס לניתוח, השתנו.
4. דווקא בתקופה שבה המשאבים מצומצמים, סקר הסיכונים יאפשר להתמקד בתחומים בהם מרוכזים הסיכונים, וכך למעשה יחסוך כסף לארגון.

Fahn Kanne Control Manegment Ltd. All rights reserved.

מי אנחנו - שירותים בתחום מערכות מידע

- ליווי ובקרה על תהליכי פיתוח המערכות וניהול הפרויקטים, בדיקת אפקטיביות הבקרות, ייעוץ והמלצות על שילוב בקרות מתאימות.
- סקר סיכונים בתחום ה- IT (תפעולי ואפליקטיבי).
- יעוץ והכנה לתאימות לרגולציות וסטנדרטים בתחום ה-IT.
- ייעוץ להכנת תוכניות ההמשכיות העסקית (BCP) וההתאוששות מאסון (DRP).
- ייעוץ בתחום אבטחת מידע.
- כתיבה וסקירה של נהלים.
- הפעלה שוטפת של מערך בקרות ה- IT העתיות.
- חקירה ואיתור הונאות באמצעות שימוש בכלים ממוחשבים.

Fahn Kanne Control Manegment Ltd. All rights reserved.

Fahn Kanne
Grant Thornton

תודה על ההקשבה

רמי ניסן, (CISA ,MBA)
מנהל מחלקת מערכות מידע
פאהן קנה ניהול בקרה
ramin@gtfk.co.il
052-3338185

Fahn Kanne Control Manegment Ltd. All rights reserved.