מבדקי חדירה ובחינת בשלות הבקרות, ככלים להעלאת רמת החוסן הארגוני

אלכס מור

יוני 2019

EY
Building a better working world

שקף 1 במצגת תקציר מנהלים

תובנות עיקריות

- חשופה כיום באופן משמעותי לאיומי סייבר חיצוניים ופנימיים, ומערך הבקרות
- הק[illegible] על נכסי המידע ותהליכיה העסקיים של החברה.
- קיים סיכון גבוה לפגיעה פ[illegible] עקב דליפת מידע פרטי ו/או
- פיננסי ושיבושים במערכות האינטרנטיות, כגון מ[illegible]
- מאחר שמערך הסייבר אינו מובנה ברצף הפעילות בחברה, יכולת ה[illegible]
- מוגבלת, דבר שעלול לגרום לשיבוש חמור בהמשכיות העסקית.

האם זה יכול לקרות בחברה שלך?

סקר הערכת בקרות

- **בקרות** הן אמצעי ההגנה אותן הארגון נדרש לממש במטרה לצמצם את הסבירות להתממשות והנזק הנגרם כתוצאה מאירועי סייבר. הבקרות כוללות תהליכים, נהלים, מערכות הגנה וטכנולוגיות.
- סיכון סייבר מתייחס להתממשות פעילות זדונית בה מעורבות תשתיות, מערכות ותוכנות מחשב אשר מובילה לנזק משמעותי לארגון ופגיעה בתהליכים העסקיים.
- מערך הבקרה אמון על ביצוע סקרים לבדיקת יעילות הבקרות בדגש על נקודות המבט של התוקף – חשיפה וניצול של סדרת חולשות אנושיות וטכנולוגיות במטרה **למקסם את הרווחים.**
- תפיסה משולבת:
  - ניתוח רמת בשלות הבקרות בהתאמה לגורמי האיום, לסקטור העסקי ולמקובל בתעשייה
  - הדמיית תקיפה של מספר מוקדי סיכון בו זמנית ובחינת יעילות הבקרות העיקריות לזיהוי, הגנה, איתור, תגובה, והתאוששות מאירועי סייבר

"קיימים שני סוגי ארגונים בעולם, כאלה שפרצו אליהם וכאלה שעדיין לא.

ואפילו הם מתכנסים לקטגוריה אחת: חברות שנפרצו וייפרצו שוב."

רוברט מולר, ראש הFBI לשעבר
מרץ 2012

סקירת מצב הגנת הסייבר בעולם ואירועים מרכזיים בישראל

סקירת חדשות

פירצה חמורה באיתוראן: פרטי לקוחות נחשפו - כולל חשבון הבנק והספרות האחרונות בכרטיס האשראי

ה לצפות בכתובות, במספרי
The סגרה החברה את האזור

224 22 שמור

"כל המידע תוך עשר שניות": פרצה חמורה חשפה פרטים פיננסיים של אלפי ישראלים ברשת

המידע שדלף מאתר iFreelance כולל הכנסות והוצאות של בתי עסק, וכן רשימות של ספקים ולקוחות עם מספרי תעודת זהות ודיווחים לפי שנת מס ■ פרצת האבטחה התגלתה במקרה על ידי לקוח, שדיווח לחברה

רפאלה גויכמן | התראות במייל
21:00 21.04.2018 | עודכן ב: 06:09 22.04.2018

137 25 שמור

נמיליוני תמונות של ילדים ופרטים של 100 אלף הורים: הדליפה הענקית מאפליקציית הגנים בישראל

רמיני היא אפליקציה המאפשרת לצוותים של גני ילדים לתקשר עם ההורים ולחלוק תמונות, מידע אישי ולוח אירועים של הגן ■ משרד החינוך המליץ על האפליקציה, אך פרצת אבטחה בה חשפה ברשת כ-6 מיליון תמונות של ילדי גן ופרטים של יותר מ-100 אלף הורים

אמיתי זיו | התראות במייל
06:00 11.03.2018 | עודכן ב: 10:23

370 53 שמור

מקורות: Globes, TheMarker

פרצת אבטחה חמורה ב... מועמדים

כשלי אבטחה חמורים התגלו באתר השב"... שגילה את הפרצה אף הוסיף לאתר את ה... המינהליים לאלתר" - ומחק אותה מיד לא...

אמיתי זיו | התראות במייל
18:17 25.04.2018 | עודכן ב: 18:50

מצב הגנת הסייבר בישראל

- עלייה עקבית בתקציבי הגנת הסייבר בארגונים, במקביל למאמצי ייעול ההגנות הקיימות והטמעת ההגנות כבר בשלב תכנון המערכת.
- מחסור בכח אדם מנוסה ומיומן ממשיך להוות מכשול משמעותי ליישום מדיניות הגנת סייבר. עקב כך, חברות רבות במשק החלו לרכוש שירותי סייבר מנוהלים.
- במרבית הארגונים קיימת מדיניות אבטחת מידע וסייבר וקיימת מודעות הנהלה לצורך לבדוק את האפקטיביות של מערך ההגנה.
- הביקורת הפנימית בוחנת ומבקרת את הניהול והיישום של מערך הגנת הסייבר.
- עלייה בחשיבות מודעות העובדים לזיהוי ומניעה של התקפות סייבר בארגון.

סקר אבטחת המידע הגלובלי EY GISS 2018-19

1,464

פקידי ממשל שהסיסמא שלהם למחשב הייתה "Password123"[1]

1,946,181,599

המספר הכולל של רשומות המכילות מידע אישי ונתונים רגישים אחרים שנחשפו בין ינואר 2017 למרץ 2018[2]

6.4 מיליארד

מספר המיילים המזוייפים הנשלחים בעולם – מדי יום[3]

41%

מהארגונים בסקר מצהירים שיש להם תוכנית חוסן מעודכנת והם עושים שימוש תדיר בכלי סריקה ותקיפה

78%

מהנשאלים מעריכים שטעויות עובדים היא המקור הסביר ביותר לתקיפת סייבר בארגון

38%

מהארגונים בסקר לא צפויים לזהות פריצה על ידי גורם איום מתוחכם או בעל אמצעים

13.5 מיליון דולר

נגנבו מהבנק ההודי Cosmos Bank. האקרים פרצו למערכות הבנק ושתלו תוכנה זדונית בכספומטים.

22%

מהארגונים רואים במתקפות פישינג כגורם איום מספר אחת

1 The Washington Post, August 22, 2018 [https://www.washingtonpost.com/technology/2018/08/22/western-australian-government-officials-used-password-their-password-cool-cool/]
2 Chronology of Data Breaches, March 2018 [https://www.privacyrights.org/data-breaches]
3 Dark Reading, August 27, 2018 [https://www.darkreading.com/endpoint/64-billion-fake-emails-sent-each-day/d/d-id/1332677]

אתגרי מערך הבקרה בהתמודדות עם איומי סייבר - הפער ההולך וגדל

איומי סייבר, הן פנימיים והן חיצוניים לארגון, גדלים בקצב מהיר יותר מהיכולת של ארגונים לממש פתרונות ושיפורים לתוכנית אבטחת המידע שלהם. בנוסף, ייתכן שארגונים לא יהיו מסוגלים להגיב בצורה אפקטיבית לאירוע של תקיפת סייבר. כל אלו גורמים לפער הולך וגדל מידי יום.

רגולציה במרחב הסייבר

- בישראל ובעולם קיימים מספר תקנים ורגולציות בנושא ניהול סיכוני סייבר ונקיטת אמצעים מתאימים לשמירה על המידע ולניהולו בצורה יעילה ולפי פרקטיקות מקובלות בעולם.
- עמידה בתקן אינה מבטיחה עמידות בפני תקיפות, אבל מוכיחה, שהארגון נוקט במאמצים לנהל את סיכוני הסייבר ואף לבחון את יעילות מערכי ההגנה, כנגד התפתחות האיומים וגילוי חולשות חדשות, שנה אחרי שנה, בניסיון למזער את הנזק.

- חוק הגנת הפרטיות
- תקנות המפקח על הביטוח
- SOX
- הוראת נב"ת (ניהול בנקאי תקין) 361 - ניהול הגנת הסייבר
- ניהול סיכוני סייבר של רשות שוק ההון
- הוראה 257
- NIST CSF
- ועוד ועוד

אבטחת מידע וסייבר כיום הינם עיסוק של כולם

מה תפקיד מערך הבקרה, בעידן התעצמות תחום הסייבר?

תפקיד מערך הבקרה

- בחינת ניהול ויישום תוכנית הגנת הסייבר וההמשכיות העסקית למול גורמי האיום, הסוגיות והסיכונים העדכניים
- הערכת בשלות בקרות הגנת הסייבר - סקרים וראיונות - People, Process, Technology
- בחינת איכות ויעילות מערכי ההגנה ורמת הטמעת הבקרות הקיימות (זיהוי, הגנה, איתור, תגובה והתאוששות) באמצעות תרגול - בדיקות חדירות, הדמיית תקיפה (Red Team), ניהול משברים
- בחינת מערך המחשוב וציוד התקשורת בעמידה ברגולציות שונות, בהמלצות היצרן ומול פרקטיקות מקובלות בתעשייה – סקר פגיעויות
- ביצוע בדיקות וביקורות יזומות לספקי משנה, TPRM

הערכת רמת אפקטיביות בקרות ההגנה בסייבר של הארגון וזיהוי הפערים

Top-down

בחינת תוכנית הגנת הסייבר הארגונית

לצורך בחינת בשלות תכנית אבטחת המידע הארגונית, שיפור רמת האפקטיביות שלה והתאמתה לעולם אבטחת המידע והסייבר המשתנה, סוקרים 20 תחומים שונים אשר מתייחסים לעולם אבטחת המידע והסייבר, אשר עבור כל אחד מתשאלים בעלי תפקידים רלוונטיים תוך התייחסות לבקרות, אמצעים ותהליכים טכנולוגיים וארגוניים, בדגש על מתן דוגמאות מהשטח.

Bottom-up

בחינת אפקטיביות הבקרות

תכנון וביצוע סקרי פגיעויות ומבדקי חדירות על אפליקציות ותשתיות הארגון במטרה לזהות פגיעויות, חולשות ונקודות כשל היכולות להוביל לפרצות. על ידי שילוב מספר מתקפות (לדוגמא, הנדסה חברתית) ניתן לקבוע את רמת יעילות הבקרות ומידת הטמעתה בארגון

בחינת תוכנית הגנת הסייבר הארגונית

לצורך הערכת בשלות הבקרות מקיימים ראיונות עם גורמים טכנולוגיים בארגון ועם גורמים נוספים, כגון היחידה לניהול סיכונים (אם יש כזאת). לכל בקרה קיימת טבלת דירוג ייחודית לה, שבמסגרתה מגדירים את סולם ההערכה של רמת הטמעת הבקרה בארגון, כאשר הציון 5 מבטא הטמעה מיטבית.

דוגמא - ניתוח בקרה למניעת קוד זדוני באמצעים טכנולוגיים, מהם הכלים ומה התנאים להפעלתם:

הערכת הטמעת הבקרה	ציון
הארגון משתמש בטכנולוגיות לא פורמליות לזיהוי נוזקות	1
זיהוי נוזקות מבוצע באמצעות תוכנות אנטיוירוס מסורתיות, מבוססות חתימות	2
לחברה כלים וטכנולוגיות מתקדמות לזיהוי נוזקות המופעלות כחלק משלבי התוכנית לטיפול באירוע סייבר	3
החברה משתמשת בטכנולוגיות מבוססות התנהגות כדי לסרוק אחר תוכנות זדוניות ונוזקות, אך לא בהכרח בסביבה כולה	4
החברה משתמשת בטכנולוגיות מבוססות התנהגות כדי לבצע סריקה מתמשכת של תוכנות זדוניות ונוזקות בכלל הסביבות של החברה	5

בחינת אפקטיביות הבקרות - סריקת פגיעויות או מבדק חדירות?

- <u>הגדרת יעדים לסריקת פגיעויות</u>
  - מערך שרתי Windows
  - בדיקת הקשחה לבסיסי נתונים
  - בחינת חוקים והגדרות ה-Firewall בהתאם למקובל בתעשייה

- <u>הגדרת יעדים למבדק חדירות</u>
  - עקיפת הגבלות לוגיות (עסקיות)
  - גישה למידע רגיש / מידע רפואי / כרטיסי אשראי / תשלומי ספקים / משכורות
  - עקיפת מערכות הגנה פיזיות (תג כניסה, שומר, דלתות)
  - הרשאות ניהול סביבת ענן
  - הרשאות ניהול Active Directory
  - הרשאות ניהול מערכות קריטיות

ממצאים עיקריים מסקרי בשלות של לקוחות

אסטרטגיית וניהול אבטחת המידע והסייבר

- לא קיימת אסטרטגיה ארגונית בנושא אבטחת מידע והגנת הסייבר.
- לא קיימת תוכנית עבודה שנתית להגנת הסייבר

ניהול סיסמאות

- מדיניות הסיסמאות אינה עומדת בסטנדרטים הקיימים היום בתעשייה והמלצות היצרן

ניהול משתמשים והרשאות

- כמות גדולה של משתמשים בעלי הרשאות גבוהות (משתמשי על).
- הגישה לרשת הארגון אינה מוגבלת בזמן.
- הרשאות רחבות במערכות שלא על פי עקרון "הצורך לדעת".
- גישה חופשית למשאבי הרשת ולתיקיות המכילות מידע רגיש.
- לכל עובד קיימת הרשאת מנהל מקומי על המחשב האישי

ארכיטקטורה

- ארכיטקטורת הרשת הארגונית אינה מיישמת הפרדה לוגית בין סביבות (סגמנטציה)

ניהול ספקים

- קיימים ספקים בעלי גישה מלאה לרשת הארגון.
- הגישה לרשת הארגון אינה מוגבלת בזמן.
- לא קיים מעקב אחר פעילות הספקים ברשת החברה.
- לספקים יש הרשאת "משתמש על" ברשת הארגונית.

גישה מבחוץ

- לא קיימת מערכת להזדהות חזקה לגורמים הניגשים מבחוץ.
- עבודה עם מחשבים שאינם מוגנים.

ניהול שינויים

- לא קיימים היבטי אבטחת מידע בתהליך ניהול השינויים

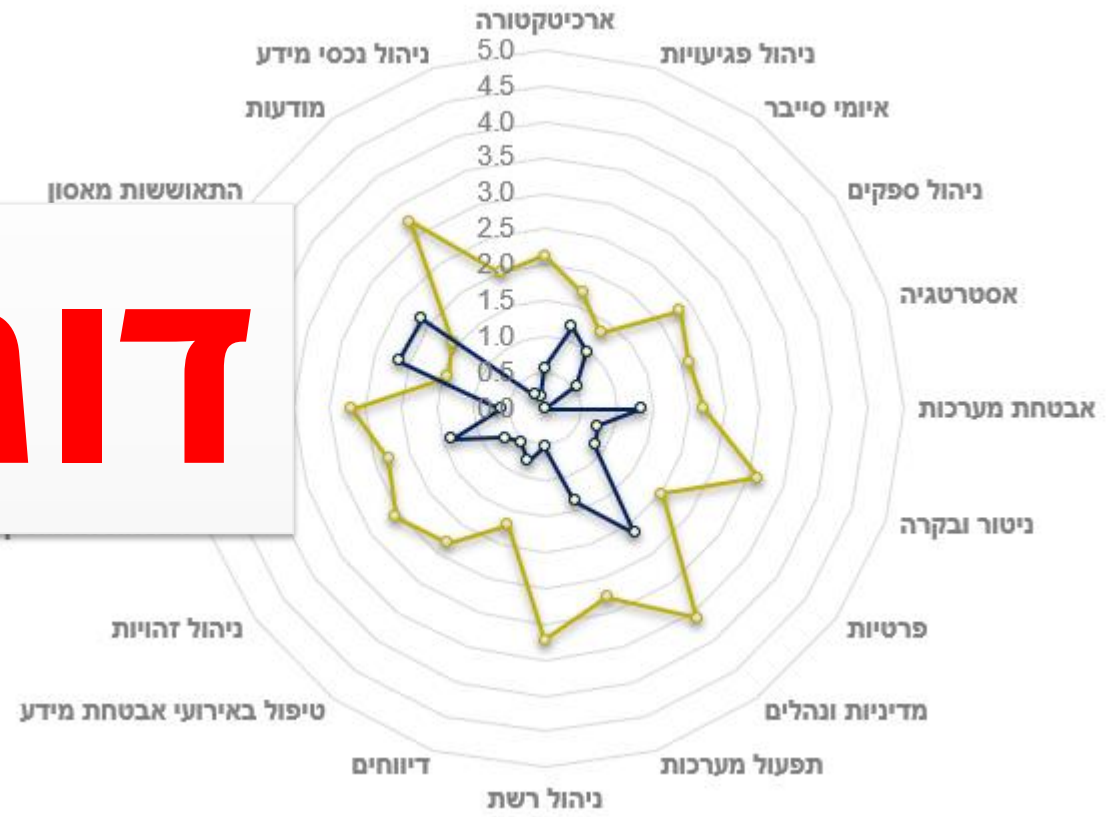
ניהול ניטור אבטחה ושימוש במדדים

- לא קיימת מערכת ניטור אבטחתי
- לא הוגדרו מדדים כמותיים לזיהוי חריגות

דוגמאות לתוצרי עבודה

תמונת מצב של בשלות מערך אבטחת המידע והגנת הסייבר של החברה למול ציון ממוצע של חברות באותו מגזר בתעשייה

תשתית אבטחה ע"פ EY	מצב נוכחי
מדדים ודיווח	2.86
ניהול שרשרת אספקה	2.95
ארכיטקטורה	3.23
מסגרת נהלים, מדיניות וסטנדרטים	3.65
נה על מידע	3.74
ול מלאי הנכסים	3.85
טיות	3.85
ול איומים ופגיעויות	3.92
ול גישה והזדהות	3.93
פעול	3.95
שתית נתונים – אירועים/התראות/לוגים	3.97
של וארגון	4.00
ניהול אירועים	4.07
אבטחה בפיתוח ותוכנות	4.18
ניטור אבטחה	4.28
מודעות	4.38
אבטחת מידע לתחנות עבודה	4.45
אסטרטגיה	4.50
אבטחת רשת	4.12



דוגמה

בדיקות חדירות אפליקטיביות

בניית תרחישי תקיפה עסקיים בדגש על האיומים המרכזיים שהארגון חשוף אליהם

- אפליקציות פנימיות (Desktop)
- אפליקציות מבוססות דפדפן (Web)
- אפליקציות לטלפונים חכמים (Mobile)
- ניתוח קוד בהיבטי אבטחת מידע
- אפליקציות SAP
- אפליקציות Mainframe

אבטחת אפליקציות

Mobile & Web – Black box, Grey box and Code Review

בדיקות חדירות לתשתיות הארגון

בדיקת מערך ההגנה כנגד שילוב מספר וקטורי תקיפה

- בדיקת חדירה לארגון מבחוץ
- בדיקת גישה והרשאות גישה מעמדת עובד
- בדיקת חדירה מתוך הארגון
- בדיקת חדירה מרשתות אלחוטיות
- בדיקות VPN
- בדיקת מערך הטלפוניה - VoIP
- בדיקת תשתיות מחשוב ענן
- בדיקת חדירת לתשתיות SCADA

בדיקות תשתית
External, Internal and Wireless, Cloud, SCADA...

קריאה נוספת

- ניהול בנקאי תקין, הוראה מס ' 310
- תורת ההגנה בסייבר לארגון - מערך הסייבר הלאומי
- קווים מנחים לניהול סיכוני סייבר - סייבר, מודיעין וביטחון

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

ED None

ey.com