21 במאי, 2024

עמדת הרשות בנושא ביצוע סקר סיכונים ומבדקי חדירות למערכות מידע

עדכוני לקוחות

ביום 9 במאי 2024 פרסמה הרשות להגנת הפרטיות (להלן: "**הרשות**") **מסמך עמדה** בנושא ביצוע סקר סיכונים ומבדקי חדירות למערכות מידע, בהתבסס על הוראות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז- 2017 ("**התקנות**"). הרשות עמדה על כך שבעוד שחובה לערוך מבדקי חדירות וסקרי סיכונים עיתיים למאגרי מידע שחלה עליהם רמת האבטחה הגבוהה על-פי התקנות, סקרי סיכונים ומבדקי וחדירות מהווים פרקטיקה רצויה לביצוע בכל ארגון וביחס לכל מאגר מידע אישי.

ריכזנו עבורכם את הנושאים המרכזיים העולים מעמדת הרשות:

כל הזכויות שמורות, גורניצקי ושות' © משרד עורכי דין

	סקר סיכונים	מבדק חדירות
מטרה	איתור סיכוני אבטחת מידע והערכת רמת הבשלות הארגונית להתמודדות עם איום לפגיעה בשלמות, סודיות וזמינות המידע בארגון. בכלל כך, סקר סיכונים הוא דרך המלך למיפוי סיכוני אבטחת המידע וקביעת דרכי ההתמודדות עימם, כנדרש במסגרת מסמך הגדרות המאגר ובמסגרת נוהל אבטחת המידע.	זיהוי וניתוח החולשות באבטחת המידע הארגונית באמצעות הדמיית מתקפה על נכסי הארגון.
תחולה	החובה חלה רק על מאגר מידע ברמת אבטחה גבוהה. יחד עם זאת, הרשות ממליצה גם לארגונים בעלי רמת אבטחת בינונית או בסיסית לבצע סקרים בהתאם לאופי המידע, רגישותו, היקפו וחשיבותו לארגון וללקוחותיו.	החובה חלה רק על מאגר מידע ברמת אבטחה גבוהה. כאמור, הרשות ממליצה על עריכת מבדק חדירות גם ביחס למאגרי מידע ברמת אבטחה בינונית או בסיסית.
תדירות	• מיד בסמוך לאחר הפעלת המאגר והקמת מערכות המאגר. • בתדירות ההולמת את הדינמיקה הטכנולוגית, העסקית והרגולטורית של הארגון, ולפחות אחת ל-18 חודשים. • בסמוך לביצוע שינויים טכנולוגיים במערכות המידע או ברכיבי מסמך ההגדרות של הארגון.	• מיד בסמוך לאחר הפעלת המאגר. • בתדירות ההולמת את הדינמיקה הטכנולוגית, העסקית והרגולטורית של הארגון, ולפחות אחת ל-18 חודשים.
תהליך ביצוע	• הגדרת נכסי הארגון על ידי ההנהלה הבכירה ומיפוי האיומים על המידע הארגוני והפעילות העסקית של הארגון במסמך הגדרות מאגר; • מיפוי מערכות מאגר המידע; • זיהוי חולשות ופגיעויות אפשריות, לרבות התייחסות לניהול התקנים ניידים; • הערכת מידת השפעת התממשות האיומים ומזעור סבירות התממשותם; • מיפוי הפעולות והבקרות הקיימות בארגון למול הפעולות והבקרות אותן ראוי ליישם והערכת הסיכון השיורי; • זיהוי ומיפוי סיכוני אבטחת המידע הכרוכים בהתקשרות עם גורם חיצוני לצורך קבלת שירות; • פירוט החשיפות שזוהו בדו"ח מרוכז.	המבדק יכול להתבצע ברמות שונות של ידע והיכרות עם נכסי הארגון: • מבדק "קופסה לבנה" – למבצע המבדק נמסר מידע רב על הארגון כדי לתכנן ולעצב את פעולותיו להמשך; • מבדק "קופסה אפורה" – למבצע המבדק נמסר מידע חלקי על הארגון כך שהארגון יוכל להפעיל שיקול דעת רחב ביחס להיקף המבדק; • מבדק "קופסה שחורה" – למבצע המבדק לא נמסר כל מידע על הארגון; • לאחר ביצוע המבדק, יש לדון בממצאי המבדק ולגבש תכנית עבודה לתיקון הליקויים.
דגשים נוספים	• בעל מאגר שחלה עליו רמת אבטחה גבוהה רשאי לקיים את החובה על-פי התקנות לערוך ביקורות תקופתית במסגרת סקר הסיכונים. • במקרה בו ארגון התוודע לסיכוני אבטחה או לשינויים במיפוי סיכוניו, עליו לפעול באופן מיידי למזעור הסיכונים ולא להמתין עד לחלוף תקופה של 18 חודשים.	• מבדק החדירות חייב להתבצע לאחר קבלת הסכמת מפורשת של האורגנים המוסמכים בארגון על מנת להימנע מביצוע עבירות.

כל הזכויות שמורות, גורניצקי ושות' © משרד עורכי דין

ביצוע סקר סיכונים ומבדק חדירות הוא חיוני מבחינה משפטית, עסקית וטכנולוגית. הוא נועד לא רק לשם עמידה בדרישות התקנות אלא גם כדי לפתח את הפעילות העסקית של הארגון ולאפשר מתן מענה מיטבי ללקוחותיו. לצד זאת, אי ביצוע סקרי סיכונים ומבדקי חדירות מקום בו חלה חובה לעשות כן, מהווה הפרה של הוראות התקנות ועלול להוביל לפתיחה בהליך אכיפה מנהלי על ידי הרשות.

אנו מזמינים אתכם לפנות אלינו לכל שאלה ו/או התייעצות בנושא.

עדכון זה הוכן בסיועה של מליסה פוירון.

* עדכון זה נועד לספק מידע כללי ותמציתי בלבד. הוא אינו מהווה ניתוח מלא או שלם של הסוגיות הנידונות, אינו מהווה חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו.

אנשי קשר

אסף הראל
שותף

רבקה גניס שפטובסקי
עורכת דין בכירה

כל הזכויות שמורות, גורניצקי ושות' © משרד עורכי דין