SANS SECURITY AWARENESS

אאוץ! | מאי 2018

עלון מודעות אבטחת מידע למשתמשי מחשב

GDPR

סקירה כללית

ייתכן ששמעת על חוק חדש שנקרא GDPR (רגולציית ההגנה על הפרטיות), או כללי ההגנה על נתונים (General Data Protection Regulation). חוק זה פותח על ידי האיחוד האירופי ונכנס לתוקף ב 25- במאי 2018. הוא חל על כל ארגון המטפל במידע האישי של כל תושב באיחוד האירופי, ללא תלות במקום שבו נמצא הארגון. GDPR דורש מארגונים לשמור על הפרטיות והאבטחה של מידע אישי של תושבי האיחוד האירופי. כדי להבטיח עמידה בGDPR, יש להבין עקרונות מפתח וליישמם.

לאנשים יש זכות לפרטיות. ארגונים צריכים לכבד את הפרטיות שלהם על ידי הגבלת הנתונים האישיים שהם אוספים, מעבדים, והדרך בה הם מאבטחים את הנתונים. חובות פרטיות חלות על כל מידע, בין אם המידע עצמו או בשימוש בשילוב עם מידע אחר, שיכול לזהות אדם החי באיחוד האירופי. מידע זה יכול לכלול פריטים כגון כתובות, מספרי דרכונים, מספרי רשיון נהיגה, פרטים פיננסיים, ביומטריה, חברויות באיגוד, היסטוריה רפואית, נתוני מיקום או מידע הנוגע לאופיו המיני, הדתי או הפוליטי של אדם. ההוראה חלה על "natural person", כלומר אדם חי. הנה כמה עיקרי התווך של GDPR כי יש לממש:

- נתונים אישיים יעובדו באופן חוקי, הוגן ובצורה שקופה.
- צריך לספר לאנשים איזה מידע נאסף ולשם איזו מטרה.
- נתונים אישיים ייאספו למטרות נוקבות מפורשות ולגיטימיות. אין להשתמש בהם שום דרך אחרת המנוגדת למטרות אלה.
- נתונים אישיים יישמרו ויעובדו כל עוד המידע נדרש למטרה שנאסף ולא יותר מזה.
- הנתונים האישיים חייבים להישמר מעודכנים ומדויקים.

לאנשים יש את הזכות לקבל עותק של הנתונים שלהם או לבקש כי לא יהיה שימוש בנתונים האישיים שלהם, או בחלק מהמקרים, למחוק לחלוטין את הנתונים.

על הארגונים לנקוט באמצעי אבטחה מתאימים כדי להגן על נתונים אישיים מפני הרס, אובדן, שינוי או חשיפה לא חוקיים או בלתי חוקיים.

בנוסף, ארגונים צריכים להבטיח שכל הצוות המטפל בנתונים האישיים מאומן כראוי כיצד לאבטח ולהגן על נתונים אלה.

אמצעי ההגנה הקיימים נועדו להבטיח ולקיים את רמת ההגנה המתאימה לרמת האופי של הנתונים האישיים והרגישים. ככל שהסיכונים הקשורים לנתונים גדלים, כך המאמץ וההוצאות של הצעדים הננקטים בהגנת הנתונים צריכים לגדול. צריכים לעדכן צעדים והגנות אלו באופן שוטף ובמידת הצורך. יש לקיים תיעוד מתועד היטב בנוגע לפרטיות, החלטות אבטחה, ואמצעים לסייע לעמידה בדרישות. בנוסף, ארגונים מחויבים מבחינה משפטית לנקוט אמצעים, כגון חוזים וביקורות נאותות, על מנת להגן על נתונים אישיים בעת העברתם לצדדים שלישיים חיצוניים ובמיוחד לאלה מחוץ לאיחוד האירופי. לבסוף, במקרה של הפרת נתונים אישית, ארגונים ידווחו על ההפרה בתוך 72 שעות לאחר שנודע להם. כישלון של ארגונים לעמוד ב- GDPR עלול לגרום לקנסות של עד 4% מההכנסה הגלובלית שלהם, מה שהופך את הGDPR לאחד התקנות העולמיות הכי יקרות בעולם.

עורך אורח

בריאן הונאן הוא מנכ"ל BH Consulting, חברת ייעוץ עצמאית להגנה על נתונים, שממוקמת בדבלין אירלנד. בריאן שימש כיועץ מיוחד ל (EC3 (Europol's Cybercrime Centre הוא מייסד ה- CERT הראשון של אירלנד, הוא יושב במועצה המייעצת למספר חברות אבטחה חדשניות. מצא את בריאן בכתובת www.linkedin.com/in/brianhonan *או בטוויטר* @brianhonan.

מקורות

סקירה כללית עבור אנשים וארגונים: http://gdprandyou.ie

תקנת GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

אאוץ! תרגומים וארכיונים: https://www.sans.org/u/D88