

Wiarygodność w cyfrowym świecie

Cyfryzacja i postęp technologiczny zmieniły sposób prowadzenia biznesu, umożliwiając firmom szerszy dostęp do klientów dzięki wielu usługom online. Jednak rosnąca zależność od technologii wiąże się z poważnymi zagrożeniami - jak wynika z raportu „Barometr Cyberbezpieczeństwa” KPMG, aż 66% przedsiębiorstw doświadczyło incydentów naruszających bezpieczeństwo w sieci.

Phishing, malware czy APT to tylko kilka metod stanowiących zagrożenie dla bezpieczeństwa polskich firm. Wyłudzeniem danych zostało dotkniętych aż jedna piąta firm. W porównaniu z badaniem sprzed roku, ataki na urządzenia mobilne i sieci bezprzewodowe, przesunęły się na wyższe miejsca, co oznacza, że przedsiębiorstwa traktują te zagrożenia znacznie poważniej. Co ciekawe, ponad jedna trzecia firm nie uważa ataków na łańcuch dostaw za istotne zagrożenie.

Inwestycje w cyberbezpieczeństwo nadal stanowią problem - firmy dostosowują wydatki zależnie od branży, wielkości i specyfiki zagrożeń. Często decyzja o nowych zabezpieczeniach wynika z konieczności adaptacji oraz utrzymania konkurencyjności w dobie dynamicznych zmian zachodzących w biznesach istniejących online.

Problemy z rekrutacją specjalistów ds. cyberbezpieczeństwa, motywuje firmy do korzystania z usług outsourcingowych. W 2023 roku już ponad 84% przedsiębiorstw podjęło decyzję o wsparciu firm zewnętrznych.

W cyberbezpieczeństwie najważniejsza jest czujność na incydenty oraz stała edukacja pracowników w celu zwiększenie ich świadomości. W obliczu rosnących zagrożeń należy odpowiednio dostosowywać nowoczesne metody ich zwalczania, by skutecznie chronić nie tylko firmę, ale również wszystkich klientów biznesowych.