

Cyberbezpieczeństwo to najważniejszy trend rynkowy w 2023 roku. Tak wskazało 78% badanych w raporcie pn. „Wpływ skutków pandemii koronawirusa na potrzeby kompetencyjne sektorów Informatyki oraz Telekomunikacji i Cyberbezpieczeństwa” zrealizowanego przez Antal. Wynika to ze zmiany modelu pracy – blisko 80% firm deklaruje zwiększone zapotrzebowanie na narzędzia pracy zdalnej. Stosowanie nowych technologii, umożliwiających pracę z każdego zakątka na świecie, wymusza wprowadzenie rozwiązań zapewniających bezpieczeństwo przetwarzanych danych.

Dodatkowym czynnikiem przyspieszającym digitalizację procesów obiegu dokumentów jest Krajowy System eFaktur, który od 2024 roku wchodzi ostatecznie w życie. Modyfikacjom będą podlegały procesy wspomagane przez systemy ERP lub systemy finansowo-księgowe. Krajowy System eFaktur niesie ze sobą nowe możliwości biznesowe związane m. in. z optymalizacją procesów biznesowych, przyspieszeniem procesów fakturowania. Jednakże z drugiej strony podnosi poprzeczkę w zakresie zapewnienia bezpieczeństwa informacji.

Digitalizacja procesów czy dostępność systemów przetwarzania z sieci publicznej naraża je na cyberzagrożenia, takie jak ataki phishingowe, złośliwe oprogramowanie, np. ransomware itp. Z tego powodu przedstawiciele firm branży nowych technologii stawiają na wdrożenie polityk bezpieczeństwa czy dobrych praktyk (73%), przygotowanie procedur bezpieczeństwa (51%) czy szkolenia pracowników z cyberbezpieczeństwa (67%).

*- W dzisiejszych czasach każda dobrze prosperująca firma musi zadbać o swoje bezpieczeństwo cyfrowe. Warto zastanowić się, w jaki sposób opracować polityki i procedury bezpieczeństwa, a następnie weryfikować ich skuteczność. Ponadto budując system bezpieczeństwa informacji, istotnym elementem będą stosowane zabezpieczenia techniczne, jak wskazywane przez 73% respondentów oprogramowanie antywirusowe i antyspamowe. Najlepszym sposobem budowy systemu zapewniającego odpowiednią ochronę przetwarzanych danych jest skorzystanie z uznanych międzynarodowych standardów, jak normy z rodziny ISO 27000 – mówi Tomasz Szczygieł, ekspert ds. cyberbezpieczeństwa DEKRA.*

Kompletne wskazówki dotyczące budowy systemu bezpieczeństwa informacji umieszczone zostały w normie ISO/IEC 27001:2022 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczenia bezpieczeństwa informacji. Norma poprowadzi każdego od wdrożenia do doskonalenia systemu bezpieczeństwa informacji zintegrowanego z procesami biznesowymi organizacji, wspierając w osiągnięciu złożonych celów strategicznych.

*Źródło: IP*