**Jak zadbać o bezpieczeństwo druku w sprzedaży detalicznej?**

**Ponad 70% detalistów uważa, że bezpieczeństwo urządzeń jest kluczowe z perspektywy zapewnienia odpowiedniego poziomu ochrony danych firmy i klientów. Przetwarzanie dużych ilości informacji, w tym danych wrażliwych, adresów czy szczegółów dotyczących płatności, wymaga wyjątkowej ostrożności. Zapewnienie im odpowiedniego poziomu bezpieczeństwa stanowi ogromne wyzwanie dla sprzedawców detalicznych w erze RODO. Pomimo ogólnej świadomości wielu cyber-zagrożeń, które czekają firmy, nieco ponad połowa przedsiębiorstw (51%) uważa, że w niewystarczającym stopniu inwestuje w bezpieczeństwo sprzętu drukującego.**

„*Dane osobowe to jeden z najbardziej wartościowych i pożądanych zasobów naszych czasów, dlatego warto pamiętać, że mogą stać się celem cyberprzestępców. Po stronie przedsiębiorców leży zapewnienie ochrony gromadzonym i przetwarzanym informacjom o konsumentach. Warto pamiętać, że przy potencjalnym wycieku danych detaliści ryzykują utratą – zarówno klienta, jak i ogólnego zaufania. Dlatego każde nowe wdrożenie rozwiązań technologicznych musi być sprawdzone i zgodne z najnowszymi standardami bezpieczeństwa IT*” – komentuje Katarzyna Idzkiewicz, ekspert Brother.

Istnieją trzy główne założenia dotyczące zapewnienia bezpieczeństwa informacji, które pomagają zadbać o zabezpieczenie procesu druku w branży detalicznej. Obejmują one zarówno bezpieczeństwo samego urządzenia, jak i przetwarzanych zasobów:

1. **Poufność (ang. Confidentiality)**

Dotyczy danych, które dla właściwego funkcjonowania przedsiębiorstwa muszą zostać udostępnione innym jednostkom – wiąże się to z koniecznością odpowiedniej weryfikacji docelowego odbiorcy, tak aby przekazywane informacje nie dostały się w niepowołane ręce. W tym celu należy zachować szczególne środki ostrożności, stosując uwierzytelnianie i proces autoryzacji, który wymaga od użytkowników zweryfikowania ich tożsamości przed uzyskaniem dostępu do jakiegokolwiek dokumentu.

1. **Nienaruszalność (ang. Integrity)**

Zapewnia gwarancję, że oprogramowanie sprzętowe urządzenia jest odpowiednio zabezpieczone i odporne na włamania oraz inne potencjalne zagrożenia zewnętrzne.

1. **Dostępność (ang. Availability)**

Zarządzanie bezpieczeństwem infrastruktury IT jest sporym wyzwaniem w przedsiębiorstwach, szczególnie gdy urządzenia podłączone do sieci są rozproszone. Drukarki, skanery i kopiarki powinny być tak samo zabezpieczone, jak pozostały sprzęt IT. Jeśli urządzenia te zostaną pominięte, istnieje ryzyko, że hakerzy wykorzystają te luki do przejęcia poufnych danych przedsiębiorstwa. Dlatego szczególnie istotne jest zapewnienie odpowiedniego poziomu bezpieczeństwa wszystkim sprzętom w sieci, aby zminimalizować prawdopodobieństwo powstania słabych ogniw w łańcuchu zabezpieczeń.

Warto zauważyć, że skuteczne wdrożenie najnowszych technologii wymaga nie tylko nakładów finansowych, ale również specjalistycznej wiedzy i doświadczenia pracowników. Z badania Brother wynika, że ponad połowa (57%) respondentów, jest zdania że w temacie bezpieczeństwa drukarek używa się zbyt skomplikowanego języka, który jest trudny do zrozumienia bez pomocy specjalisty. Wielu detalistów ze środowiska MŚP w codziennej pracy polega na urządzeniach i programach, które nie wymagają nadmiernego nakładu finansowego. Dlatego tak ważne jest, aby technologia wspierająca bezpieczeństwo przedsiębiorstw była łatwa w obsłudze dla użytkownika, co pomoże sprawnie zarządzać poziomem ochrony danych przetwarzanych przez firmę.