# Zalecenia dotyczące zabezpieczania urządzeń końcowych w świetle nowych wymogów.

Ogólne rozporządzenie UE w sprawie ochrony danych nakłada na przedsiębiorstwa wymóg wdrożenia środków technicznych i organizacyjnych w celu zabezpieczenia danych osobowych oraz powiadamiania odpowiednich osób i organów, jeśli naruszenie bezpieczeństwa wiąże się z danymi osobowymi.

Przedsiębiorstwa mogą więc mieć trudność ze znalezieniem czasu i zasobów, aby wywiązywać się z wymogów w terminie.

Jeżeli jednak nie zaproponują lepszych zabezpieczeń poza zwykłą zaporą w celu ochrony przed atakami cyberprzestępców, mogą paść ofiarą ataku oraz być narażone na milionowe kary. Istnieje prawdopodobieństwo, że każde przedsiębiorstwo prędzej czy później stanie się ofiarą cyberataku, dlatego też kluczowa jest identyfikacja takiego zdarzenia i natychmiastowa reakcja przy pomocy odpowiednich urządzeń, procesów i narzędzi.

Poniższa lista została przygotowana z myślą o osobach, które chcą poprawić bezpieczeństwo IT oraz uniknąć kosztownych konsekwencji naruszenia bezpieczeństwa danych. Rozpoczynając od podstawowych zasad, przechodź kolejno do listy najbardziej zaawansowanych poziomów bezpieczeństwa, dzięki czemu możesz mieć pewność, że Twoje urządzenia drukujące są zabezpieczone, a firma spełnia wymogi regulacji GDPR.

# Praktyczna lista ułatwiająca zabezpieczenie sieciowych urządzeń końcowych.

## Podstawowy poziom zabezpieczeń

- Kupuj wyłącznie urządzenia z wbudowanymi zabezpieczeniami i zaszyfrowanymi dyskami twardymi
- Aktualizuj oprogramowanie układowe, w szczególności instaluj wersje z krytycznymi poprawkami – podobnie, jak robisz to w przypadku aplikacji na smartfonie
- Skonfiguruj interfejsy urządzeń i zablokuj protokoły, takie jak FTP i telnet, które nie są wymagane przez aplikacje
- Przejrzyj nowe urządzenia i zamknij porty lub protokoły, które nie są używane, a które mogłyby ułatwić dostęp hakerom
- Wykorzystuj unikalne hasła administracyjne dla każdego urządzenia
- Zablokuj pulpit, aby uniemożliwić dostęp do funkcji administracyjnych
- Szyfruj dane wysyłane i odbierane przez urządzenie
- Ustal procedury usuwania starych danych z twardego dysku – w szczególności na drukarkach, które oddajesz do sklepu, aby otrzymać nowy produkt

Po wykonaniu tych wszystkich kroków przejdź do następnej warstwy zabezpieczeń.

## Średni poziom zabezpieczeń

- Zintegruj dane dziennika zdarzeń systemu z narzędziem SIEM, aby jeszcze lepiej monitorować sieć pod kątem zagrożeń. W świetle nowych regulacji zgodnościowych, widoczność jest kluczem do spełnienia wymogów w zakresie zgłaszania naruszeń
- Aktywuj funkcję identyfikacji użytkownika drukarki, aby monitorować, kto używa funkcji kopiowania, skanowania i faksu dostępnych w tym urządzeniu. Dane te są pomocne podczas postępowania wyjaśniającego przypadki naruszenia bezpieczeństwa danych.
- Aktywuj funkcję bezpiecznego drukowania (pull printing), aby zapobiec zapominaniu o dokumentach, zawierających wrażliwe dane. Funkcja ta przyczynia się także do wspierania standardów prośrodowiskowych Twojej organizacji poprzez ograniczanie odpadów

Po wykonaniu tych wszystkich kroków przejdź do ostatniej warstwy zabezpieczeń.

## Zaawansowane zabezpieczenia

- Wprowadź funkcję monitoringu korzystania z urządzenia i licznika wydruków
- Rozważ wprowadzenie i automatyczne egzekwowanie zasad dotyczących tego, kto i dlaczego może korzystać z danej drukarki dzięki funkcji autoryzacji na podstawie roli użytkownika
- Wykorzystuj unikalne certyfikaty cyfrowe dla każdej drukarki, podobnie jak w przypadku innych urządzeń podłączonych do Internetu w Twojej sieci
- Wykorzystuj rozwiązania druku mobilnego w odniesieniu do szyfrowania danych, dostępu do urządzeń sieciowych, identyfikacji użytkownika i monitorowania

4AA7-1093PLE