CYBERBEZPIECZEŃSTWO W DRUKU WIELKOFORMATOWYM

Technologia SmartShield chroni inżynierów przed włamaniem i kradzieżą danych

JESTEŚMY DLA INŻYNIERÓW

WIZJA CANON

- **Wierzymy w innowację** – rozwijanie nowych pomysłów i idei w celu tworzenia użytecznych i praktycznych rozwiązań.
- **Wspieramy i zachęcamy do rozwijania kreatywności** we wszystkich organizacjach na każdym etapie procesu tworzenia poprzez wizualizację pomysłów, procesów oraz końcowych projektów.
- **Kompleksowo w systemie one-stop-shop** dostarczamy naszym klientom rozwiązania wielkoformatowe: drukarki, skanery, składarki, podłoża do druku, materiały eksploatacyjne, a także oprogramowanie do wydajnego przepływu pracy. To oznacza, że wszystkie elementy są ze sobą ściśle połączone i dopasowane i od początku konstruowane tak by stanowiły jedność. Działy serwisu i wsparcia są wyspecjalizowane i skoncentrowane na tym by nasze rozwiązania działały sprawnie i wydajnie zawsze wtedy kiedy tego potrzebujesz.

Canon

CYBERBEZPIECZEŃSTWO W DRUKU WIELKOFORMATOWYM

Zagrożenia związane z atakiem informatycznym rosną z roku na rok. Nic zatem dziwnego, że bezpieczeństwo sieciowe to temat coraz częściej poruszany w biznesie. W przypadku profesjonalnego druku wielkoformatowego, na przykład podczas tworzenia dokumentacji inżynieryjnej, bezpieczeństwo i poufność danych to absolutna podstawa.

Dlatego właśnie powstał **Canon SmartShield** – inteligentny system ochrony wielkoformatowych ploterów.

CZYM JEST SMARTShield?

Pakiet zabezpieczeń **SMARTShield** rozwiązuje problemy związane z bezpieczeństwem dokumentów technicznych zawierających poufne informacje.

Bardziej niż kiedykolwiek firmy i organizacje mające drukarki wielkoformatowe muszą chronić najważniejsze, poufne i wrażliwe informacje w swoich biurach i sieciach komputerowych.

Obejmuje to informacje przesyłane z poszczególnych stacji roboczych i innych urządzeń do systemu wielkoformatowego, a także dane przechowywane w ploterze. Istotne jest też, aby systemy były chronione przed nieuprawnionym dostępem do danych do druku, drukowanych informacji i własnej infrastruktury IT, za pośrednictwem drukarek.

SMARTshield

Współczesne biura to dziś prawdziwe kłębowisko przenikających się wzajemnie powiązań. Mowa nie tylko o relacjach międzyludzkich, ale przede wszystkim o sieciach informatycznych. Wystarczy rozejrzeć się wokół - komputery, smartfony, kamery, skanery, drukarki. Każde z tych urządzeń posiada swój elektroniczny mózg oraz możliwość podłączenia się do sieci. A to niesie za sobą zarówno wiele możliwości, jak i zagrożeń.

Ochraniając swój komputer osobisty, nie możemy jeszcze czuć się bezpiecznie. Trzeba pamiętać, że urządzenia zewnętrze są równie narażone na ataki hakerów. Przedostając się do drukarki czy kamery, cyberprzestępca może wykraść wiele ważnych informacji, zablokować firmowe systemy, a nawet wykraść pieniądze albo dopuścić się szantażu.

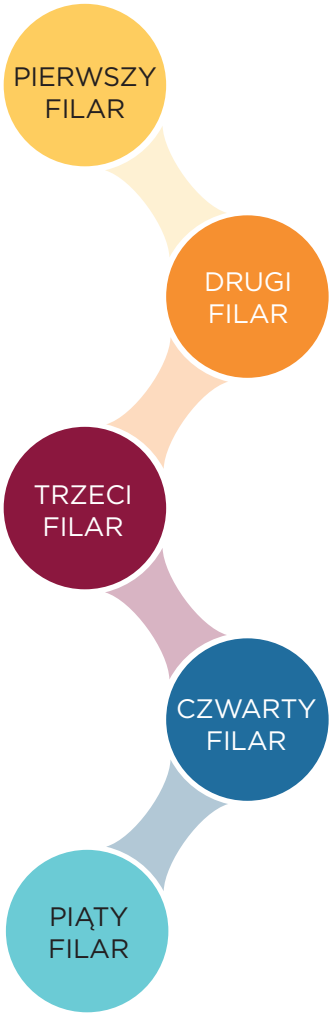
Stawka jest tym wyższa, im większe budżety wchodzą w grę. Zwłaszcza profesjonalny druk techniczny wiąże się zazwyczaj z dużymi pieniędzmi oraz wysokim poziomem poufności. Dlatego urządzenia do druku inżynieryjnego powinny być szczególnie dobrze zabezpieczone. Czy możemy ufać ich dostawcom?

PIĘĆ FILARÓW BEZPIECZEŃSTWA DANYCH

Każdego roku Komisja Europejska ogłasza październik Europejskim Miesiącem Cyberbezpieczeństwa. W sezonie 2020 z akcją zbiegła się w czasie premiera aż ośmiu nowoczesnych ploterów wielkoformatowych **ColorWave** i **PlotWave**, przeznaczonych do użycia głównie w biurach geodezyjnych, architektonicznych oraz w inżynierii produkcji. Ploter dla projektanta musi być przede wszystkim bezpieczny, dlatego właśnie ochrona sieciowa była przy konstruowaniu nowych serii absolutnie kluczową kwestią.

Zawarty w nich zestaw najnowocześniejszych rozwiązań z zakresu bezpieczeństwa nazywa się zbiorczo pakietem **SmartShield**. To pięć filarów bezpieczeństwa danych, stosowanych na każdym etapie pracy z dokumentacją wielkoformatową

PIERWSZY FILAR TO BEZPIECZNA TRANSMISJA. Praca urządzenia w trybie sieciowym to kluczowy moment, który może się wiązać z największym ryzykiem. Dlatego nowe plotery wielkoformatowe korzystają z nowoczesnych protokołów bezpiecznej transmisji danych.



DRUGI FILAR TO BEZPIECZNE PRZECHOWYWANIE. Oprogramowanie ploterów umożliwia automatyczne usuwanie plików z pamięci po czasie zadeklarowanym przez użytkownika. Dane szyfrowane są według najlepszych standardów, a przy pracy ze szczególnie poufnymi dokumentami, można zastosować technologię wyjmowanego dysku twardego. Może on zostać wyjęty i schowany w bezpieczne miejsce, na przykład do sejfu. Jego ponowna instalacja trwa chwilę i nie powinna nastręczać trudności.

TRZECI FILAR TO WIELOPOZIOMOWA AUTORYZACJA UŻYTKOWNIKÓW. Dzięki zastosowaniu tego rozwiązania, niepowołany użytkownik nie będzie w stanie uruchomić panelu maszyny. Dostęp do urządzenia może odbywać się na trzy sposoby: dzięki logowaniu do **SMART inbox** – osobistej skrzynki przechowującej dokumenty w pamięci urządzenia, przez specjalne konto w firmowej sieci zarządzania drukiem, lub dzięki dostępowi do nowoczesnej technologii chmurowej **uniFLOW**.

CZWARTY FILAR TO ZABEZPIECZENIE PRZED NIEAUTORYZOWANYM DOSTĘPEM. Innymi słowy – wyjście naprzeciw sposobom wykorzystywanym przez cyberprzestępców. W ramach czwartego filaru mieści się blokowanie niewykorzystywanych protokołów, zabezpieczenie sieci poprzez protokół SNMP czy współpraca z oprogramowaniem antywirusowym.

PIĄTY FILAR TO CIĄGŁA WSPÓŁPRACA Z DOSTAWCĄ, wykraczająca daleko poza moment kupna urządzenia. To gwarancja ciągłych aktualizacji oprogramowania, zdalnego serwisu oraz możliwości uzyskania wsparcia technicznego od producenta urządzenia.

75% WIĘCEJ OCHRONY

Tematy bezpieczeństwa sieciowego od lat stanowią podstawę konstruowanych przez Canon urządzeń wielkoformatowych. Teraz, dzięki wykorzystaniu najnowocześniejszych standardów i technologii, ochrona użytkownika może być jeszcze pełniejsza. Pakiet SmartShield zapewnia aż o 75% więcej funkcjonalności związanych z bezpieczeństwem w porównaniu do rozwiązań stosowanych w poprzednich generacjach ploterów wielkoformatowych.

Aby uświadomić wagę zagadnienia, warto przypomnieć jeden z najciekawszych ataków hakerskich ostatnich lat: w 2018 roku 50 tys. drukarek na całym świecie znienacka wydrukowało ulotkę reklamową jednego ze znanych kanałów YouTube. To akcja, która dobitnie uświadomiła wielu użytkownikom, jak łatwo włamać się do źle zabezpieczonej drukarki. Atak na firmę inżynieryjną byłby zapewne mniej żartobliwy, dlatego eksperci coraz częściej przekonują, że w każdej firmie kluczowe powinno być korzystanie z nowoczesnych rozwiązań od sprawdzonych dostawców. A poradnik kupującego ploter powinien rozpoczynać się od słów: „pamiętaj o bezpieczeństwie".

ROS