*Warszawa, 23.10.2025 r.*

**INFORMACJA PRASOWA**

**Blackout testem dla handlu. Kto przetrwa bez zasilania?**

**Nawet drobna awaria zasilania potrafi wywołać poważne skutki — zakłócenia w systemach, przestoje, a nawet straty sięgające 17 proc. rocznych przychodów[[1]](#footnote-2). Tym większe zagrożenie stanowi blackout na dużą skalę, jak ten, który sparaliżowł Hiszpanię i Portugalię. Podobne zdarzenia miały miejsce też w Pradze i Wiedniu, gdzie lokalne awarie zakłóciły funkcjonowanie transportu miejskiego oraz codzienne życie mieszkańców. Przerwy w dostawie prądu dotyczą także handlu. Uderzają w sklepy na wielu poziomach: od kas i terminali, przez magazyny, po obsługę klienta. Jak branża handlowa radzi sobie w takich sytuacjach? Czy klienci mają się czego obawiać? I co mogą zrobić detaliści, by lepiej zabezpieczyć się na przyszłość? Tłumaczy ekspert z Exorigo-Upos.**

Pod koniec kwietnia doszło do gwałtownego załamania sieci energetycznej w Hiszpanii. W ciągu kilku sekund z systemu zniknęło 15 gigawatów mocy, co sparaliżowało znaczną część Półwyspu Iberyjskiego. Z podobnymi problemami, choć na mniejszą skalę, mierzyliśmy się również na naszym podwórku. W czasie pandemii COVID-19, gdy miliony osób przeszły na pracę i naukę zdalną, gwałtownie wzrosło zużycie energii. W wielu regionach kraju pojawiały się lokalne, kilkugodzinne przerwy w dostawie prądu.

– *Do blackoutu może dojść z różnych przyczyn: awarii technicznych, przeciążenia sieci czy rosnącej liczby cyberataków, które w ostatnim czasie obserwujemy także w Polsce. Wśród kluczowych zagrożeń są też zjawiska atmosferyczne – zwłaszcza długotrwały brak opadów. Niski poziom wód w rzekach utrudnia chłodzenie elektrowni, co latem, przy wysokim zapotrzebowaniu na energię, może prowadzić do przeciążeń i konieczności czasowego odłączania odbiorców. Również powodzie i inne ekstremalne zjawiska pogodowe – jak te, które wystąpiły w ubiegłym roku na południowym zachodzie kraju – mogą powodować lokalne zakłócenia* – mówi **Michał Tomaszewski**, CISO, szef Zespołu ds. Bezpieczeństwa w Exorigo-Upos.

Dodatkowym czynnikiem ryzyka pozostają zjawiska sejsmiczne. W lipcu tego roku na Kamczatce doszło do silnego trzęsienia ziemi, po którym wystąpiło tsunami. Według wstępnych informacji, skutkiem żywiołu były przerwy w dostawach prądu w części regionów nadbrzeżnych Rosji i Japonii. Incydenty te pokazują, że skala zagrożenia blackoutem nie jest wyłącznie kwestią lokalną czy europejską.

W ostatnim czasie odnotowano też nowe, duże awarie energetyczne w Europie. Na północy Portugalii doszło we wrześniu do blackoutów, które pozbawiły prądu ponad 80 tys. osób[[2]](#footnote-3). Również w stolicy Niemiec miał miejsce potężny blackout — policja wskazała, że w tle mogą występować motywy o podłożu politycznym.

W przypadku nagłego blackoutu skutki są odczuwalne natychmiast. Awaria zasilania prowadzi do paraliżu kluczowej infrastruktury – ludzie mogą utknąć w windach, wagonach metra, czy budynkach wyposażonych w systemy automatycznego zamykania drzwi, bez możliwości szybkiej ewakuacji. Równocześnie przestaje działać sygnalizacja świetlna, co prowadzi do chaosu komunikacyjnego, zwiększa ryzyko wypadków i znacząco opóźnia działania służb ratunkowych. Problemy potęguje utrata łączności. Stacje bazowe telefonii komórkowej działają jedynie przez krótki czas na zasilaniu awaryjnym, po czym dochodzi do zaniku zasięgu i braku dostępu do internetu mobilnego.

Blackout nie pozostaje również bez wpływu na handel. W przypadku awarii zasilania klienci mogą utknąć w sklepach. Mimo to sieci handlowe dysponują procedurami awaryjnymi oraz odpowiednimi środkami bezpieczeństwa, które pozwalają na sprawne zarządzanie taką sytuacją.

To jednak tylko jedna strona problemu. Co z osobami, które właśnie próbowały zapłacić, nie mając przy sobie gotówki? W momencie przerwy w dostawie prądu terminale płatnicze i aplikacje bankowe przestają działać. W efekcie osoby korzystające wyłącznie z płatności elektronicznych stają się bezradne – czy transakcja doszła do skutku?

– *Przede wszystkim należy mocno podkreślić, że zarówno konsument, jak i jego środki w takiej sytuacji są w pełni bezpieczne –* uspokaja **Robert Andrukiewicz**, Członek Zarządu Fiserv Polska. – *W zależności od konkretnej sytuacji, np. kiedy dokładnie nastąpiło wyłączenie zasilania, możliwych jest kilka różnych scenariuszy realizacji transakcji. W przypadku, gdy terminal płatniczy potwierdził transakcję możemy być pewni, że płatność została przyjęta przez nasz bank i powinno nastąpić wydanie towaru lub realizacja usługi. W przypadku braku takiego potwierdzenia należy rozważyć alternatywną metodę płatności. Przy czym w bardzo wyjątkowych okolicznościach nasz bank mógł przyjąć płatność, ale taka informacja nie zdążyła trafić do terminala. W tej i podobnych sytuacjach konsument może zawsze skorzystać z procedury tzw. chargebacku, czyli zgłosić do banku roszczenie o pełen zwrot niezasadnie pobranej kwoty z rachunku karty.*

**Pakiet antyblackoutowy**

W odpowiedzi na zagrożenie blackoutami Polskie Sieci Elektroenergetyczne (PSE) przedstawiły tzw. „pakiet antyblackoutowy”. Dokument zawiera 21 rekomendacji podzielonych na trzy obszary: zarządzanie systemem energetycznym, cyberbezpieczeństwo oraz komunikacja ze społeczeństwem. Zmiany wymagają nowelizacji prawa energetycznego i zostały skierowane do konsultacji społecznych. Rząd wskazuje bezpieczeństwo energetyczne jako jeden z priorytetów oraz planuje inwestycje infrastrukturalne. PSE podpisały z BGK umowę na ponad 10,8 mld zł z Funduszu Wsparcia Energetyki, finansowanego z KPO. Plan zakłada budowę ponad 5 tys. km linii przesyłowych w ciągu najbliższych 10 lat, co ma poprawić stabilność systemu energetycznego oraz umożliwić przyłączanie nowych źródeł OZE i elektrowni jądrowej.

**Blackout w handlu – jak zminimalizować ryzyko strat?**

W obliczu rosnącego zagrożenia blackoutami firmy powinny zakładać, że najgorszy scenariusz jest realny – i odpowiednio się do niego przygotować. Kluczowe znaczenie mają zarówno technologie zabezpieczające infrastrukturę, jak i jasno określone procedury reagowania na sytuacje kryzysowe.

Podstawą ochrony danych jest tworzenie automatycznych kopii zapasowych w **chmurze**. Rozwiązania typu cloud backup oraz systemy odzyskiwania danych pozwalają na szybki dostęp do informacji nawet w przypadku utraty lokalnej infrastruktury. Co istotne, dostawcy usług chmurowych dysponują własnymi systemami zasilania awaryjnego i dodatkowymi centrami danych, co znacząco zwiększa bezpieczeństwo.

Firmy posiadające własne serwery powinny rozważyć **przeniesienie części zasobów do zewnętrznych centrów danych** lub **wdrożenie modelu hybrydowego**. Profesjonalne serwerownie oferują zaawansowane systemy UPS oraz wysokowydajne agregaty prądotwórcze, chłodzenie i zabezpieczenia fizyczne, które minimalizują ryzyko przestojów.

Warto rozważyć inwestycje w urządzenia, które podtrzymają zasilanie w razie awarii prądu, takie jak **zasilacze awaryjne UPS**, które natychmiast przełączają urządzenia na zasilanie bateryjne. Dzięki temu kluczowa infrastruktura IT może zostać bezpiecznie wyłączona lub działać przez krótki czas, co bywa decydujące dla ciągłości operacji. Uzupełnieniem są **stacje EPS**, które zapewniają dostawę energii elektrycznej, wystarczającą do podtrzymania pracy mniej krytycznych urządzeń, takich jak drukarki czy chłodziarki, do momentu przywrócenia zasilania.

– *Sama technologia to za mało. Równie ważne są scenariusze awaryjne i gotowe procedury działania. Każda firma powinna mieć opracowany plan na wypadek blackoutu, obejmujący nie tylko kwestie techniczne i bezpieczne wyłączanie systemów, ale też zasady pracy zdalnej, ewakuacji i komunikacji kryzysowej. Kluczowe jest również regularne testowanie tych procedur i sprawdzanie niezawodności sprzętu, bo samo wdrożenie to dopiero początek* – dodaje **Michał Tomaszewski**.

W erze powszechnej cyfryzacji blackouty przestają być wyłącznie problemem sektora energetycznego – stają się realnym zagrożeniem dla ciągłości działania firm. Prąd to dziś nie tylko źródło światła, ale fundament funkcjonowania przedsiębiorstwa. Gotowość na przerwy w dostawie prądu powinna być integralnym elementem każdej nowoczesnej strategii bezpieczeństwa biznesowego.

1. [Blackout w firmie - 3 sposoby na przetrwanie braku zasilania elektrycznego - Infor.pl](https://mojafirma.infor.pl/wiadomosci/5442943%2CBlackout-w-firmie-3-sposoby-na-przetrwanie-przerwy-w-dostawie-pradu.html) [↑](#footnote-ref-2)
2. https://podroze.gazeta.pl/podroze/7%2C114158%2C32243333%2Ceuropejski-region-spowila-ciemnosc-dziesiatki-tysiecy-osob.html [↑](#footnote-ref-3)