Plany awaryjne pracodawców, czyli jak przygotować firmę na nadzwyczajne sytuacje

PROCEDURY Ostatnia inwazja dronów unaoczniła, że **zakłady pracy muszą się przygotować na kryzysowe wydarzenia,** które mogą wpływać na ich funkcjonowanie i bezpieczeństwo zatrudnionych

Patrycja Otto
patrycja.otto@infor.pl

– Coraz częściej mamy do czynienia z nieprzewidzianymi incydentami. To czas, by zweryfikować gotowość firmy do działania w nagłych czy nadzwyczajnych sytuacjach. Właściwe rozeznanie zasobów i opracowanie procedur bezpieczeństwa oraz stworzenie systemu komunikacji z pracownikami ułatwi funkcjonowanie firmy w czasie takich zdarzeń – podkreśla Marcin Stanecki, główny inspektor pracy, apelując do pracodawców o przygotowanie się na sytuacje kryzysowe.

Eksperci od prawa pracy zapytani przez DGP podpowiadają, jakie działania należy podjąć.

Etap 1 Ocena ryzyka

Należy zacząć od analizy ryzyka, czyli określenia potencjalnych zagrożeń i kryzysów, które mogą dotknąć firmę. Na tej podstawie należy ocenić obszary działalności i kluczowe procesy, które mogą zostać przez nie sparaliżowane. Z całości analizy powinien zostać sporządzony raport wskazujący potencjalne konsekwencje dla zakładu pracy i pracowników.

Etap 2 Zmiany w regulaminach

Wszystkie wewnętrzne regulacje powinny odpowiadać zidentyfikowanym zagrożeniom. W tym zakresie na pewno nie warto korzystać z gotowców dostępnych w sieci ani ograniczać się do dokumentów do szuflady.

– Dobra procedura musi być zrozumiała dla odbiorców, czyli być dostosowana do profilu pracownika. Powinna krok po kroku określać, jak należy działać w danej sytuacji awaryjnej. Na przykład jak zachować się w trakcie pożaru, awarii sieci elektrycznej, cyberataku, incydentu bezpieczeństwa informacji. Pamiętajmy, że w dzisiejszych czasach zagrożenia logistyczne, informatyczne mogą wywołać tak samo, jeśli nie dalej idące szkody dla organizacji jak zagrożenia fizyczne – zaznacza Agata Majewska, radca prawny w TDJ Legal Morawiec.

Doktor Katarzyna Kalata, radca prawny w Kancelarii Kalata, podpowiada, że regulaminy powinny obejmować m.in. sposób alarmowania i ewakuacji, komunikację kryzysową, zasady awaryjnej pracy zdalnej lub zmiany czasu pracy, a także wyznaczenie osób odpowiedzialnych za te działania. Zmiany należy skonsultować z pracownikami lub związkami zawodowymi, a następnie ogłosić je z wyprzedzeniem, np. dwa tygodnie przed wejściem w życie.

Jak zauważa dr Magdalena Zwolińska, adwokat, partner w Kancelarii HRLS, zmiany obejmujące tryb pracy zdalnej i elastycznych godzin pracy ograniczą ryzyko związane z przemieszczaniem się oraz wprowadzą zasady pracy w sytuacjach nadzwyczajnych i kryzysowych.

Eksperci podpowiadają, by przy tej okazji zweryfikować, jak działa w firmie praca zdalna, kiedy możemy polecić ją pracownikowi i jakie warunki muszą być spełnione. Warto przyjrzeć się też temu, jakie rozwiązania w sytuacjach szczególnych przewiduje kodeks pracy. To chociażby przestój, zwolnienia od pracy z powodu siły wyższej, polecenie pracy zdalnej, warunki zlecania pracy w nadgodzinach itp. – i zaimplementować je do realiów firmy.

– Istnieje możliwość wprowadzenia równoważnego czasu pracy lub przerywanego czasu pracy – przy spełnieniu warunków określonych w k.p., ale też skrócenie okresów odpoczynku dobowego i tygodniowego czy wydłużenie okresu rozliczeniowego czasu pracy, co pozwala na większą elastyczność w organizacji czasu pracy i rozliczaniu godzin nadliczbowych – wylicza Agata Majewska.

Doktor Katarzyna Kalata dodaje, że w sytuacji nadzwyczajnej można np. polecić pracę w nadgodzinach ponad normalne limity, jeśli wymaga tego ochrona życia, zdrowia lub mienia (np. usunięcie awarii). Dopuszczalne jest też tymczasowe zmienienie grafiku pracy lub powierzenie pracownikom innych zadań niż zwykle, by utrzymać ciągłość działania firmy. Oczywiście, nawet w kryzysie trzeba zachować minimalne okresy odpoczynku i przestrzegać podstawowych zasad BHP.

Doktor Magdalena Zwolińska podpowiada też zaktualizowanie regulaminu bezpieczeństwa i higieny pracy o procedury na wypadek zagrożeń związanych z kryzysami zewnętrznymi oraz przeprowadzenie audytów wewnętrznych regulacji dotyczących ochrony danych i działań przeciw cyberzagrożeniom.

– Masowe zmiany regulaminów nie mają większego sensu, bo co do zasady wymagają uzgodnień i odbierają organizacji elastyczność. Znacznie skuteczniejszy jest przegląd już istniejących procedur oraz ich aktualizacja tak, aby były jasne i dostępne. Dobrym rozwiązaniem są także dodatkowe polityki, np. w sprawie urlopów awaryjnych czy elastycznego czasu pracy, które mogą być szybko wdrożone i dają ludziom poczucie bezpieczeństwa – podpowiada Robert Stępień, radca prawny, partner PCS Paruch Chruściel Stępień Kanclerz.

Oprócz wdrożenia wewnętrznych regulacji ważne jest również ich przetestowanie w praktyce poprzez ćwiczenia i szkolenia – np. próby ewakuacji, testy penetracyjne (np. symulowane ataki), szkolenia pierwszej pomocy.

Etap 3 Plany awaryjne

Następnym krokiem jest opracowanie planu awaryjnego i ciągłości działania.

Kompleksowy plan awaryjny powinien zawierać różne scenariusze działania w sytuacjach kryzysowych, takich jak ewakuacja lub zamknięcie firmy – w szczególności zakładów produkcyjnych, przedsiębiorstw o istotnym znaczeniu dla gospodarki, ale również w zakładach, gdzie praca musi odbywać się na miejscu oraz tych zapewniających podstawowe produkty czy usługi. Na wypadek przejścia na pracę zdalną.

– Przydatnym dokumentem jest plan ciągłości działania organizacji, który niestety funkcjonuje w stosunkowo niewielu firmach, a określa scenariusze kryzysowe i procedury reagowania, w tym role i obowiązki poszczególnych osób na wiele niespodziewanych zdarzeń i zagrożeń w firmie. Jeżeli pojawiają się nowe ryzyka – militarne, cybernetyczne, logistyczne, ale również naturalne – pracodawca powinien je uwzględnić w politykach bezpieczeństwa – zaznacza Agata Majewska.

Na tym etapie, jak wskazują eksperci, należy też zaplanować możliwość pracy zdalnej i przygotować infrastrukturę do bezpiecznego zdalnego dostępu.

– Zgodnie z art. 67^{19} par. 3 kodeksu pracy praca zdalna może być wykonywana na polecenie pracodawcy w okresie obowiązywania stanu nadzwyczajnego, stanu zagrożenia epidemicznego albo stanu epidemii oraz w okresie trzech miesięcy po ich odwołaniu. Albo też w okresie, w którym zapewnienie przez pracodawcę bezpiecznych i higienicznych warunków pracy w dotychczasowym miejscu pracy pracownika nie jest czasowo możliwe z powodu działania siły wyższej, jeżeli pracownik złoży bezpośrednio przed wydaniem polecenia oświadczenie w postaci papierowej lub elektronicznej, że posiada warunki lokalowe i techniczne do wykonywania pracy zdalnej – informuje Magdalena Zwolińska.

Jak dodaje Agata Majewska, plan awaryjny musi być też stworzony na wypadek przerwania łańcucha dostaw lub komunikacji, cyberataku lub awarii systemów IT, czy konieczności przechowywania i ochrony danych w warunkach ograniczonego dostępu do siedziby.

Etap 4 Szkolenia i komunikacja z pracownikami

Kolejny krok to przeszkolenie pracowników, by wiedzieli, jak reagować i kogo powiadomić. Warto też organizować próbne alarmy i ewakuacje, żeby przećwiczyć procedury. Dlatego ważne jest przeprowadzenie szkoleń i poinformowanie pracowników o nowych procedurach, zasadach pracy zdalnej, planie awaryjnym oraz warsztatów z zakresu pierwszej pomocy i zachowania bezpieczeństwa. Poza tym należy zadbać o zapewnienie dostępu do materiałów i wsparcia technicznego oraz ustalić kanały komunikacji kryzysowej i regularną aktualizację sytuacji.

– Pracownicy powinni wiedzieć nie tylko, gdzie jest najbliższe wyjście ewakuacyjne, ale też do kogo zadzwonić, gdy system IT przestanie działać, albo jak zabezpieczyć sprzęt w razie nagłej potrzeby opuszczenia biura. Warto upewnić się, że procedury ewakuacji są aktualne i jasno wskazują trasy, miejsca zbiórek i osoby koordynujące. To elementy, które często traktuje się jako formalność, a w rzeczywistości budują poczucie bezpieczeństwa. Krótkie, regularne ćwiczenia dają ludziom pewność i zmniejszają stres. Podobnie proste scenariusze na wypadek przerwy w dostawie prądu czy cyberataku pozwalają uniknąć paraliżu i działają uspokajająco – informuje Kinga Ciosk, starsza prawniczka w PCS Paruch Chruściel Stępień Kanclerz. Dodaje, że należy też zadbać o gotowość do szybkiego przekazywania pracownikom komunikatów rządowych czy decyzji służb oraz wyznaczenie osób odpowiedzialnych za tłumaczenie ich na proste, zrozumiałe instrukcje dla pracowników. Dobrze jest również mieć opracowane plany zastępstw czy backupowe zespoły.

Więcej na
www.gazetaprawna.pl

– Pracodawcy powinni też pamiętać, by regularnie i transparentnie komunikować pracownikom status sytuacji i działania podejmowane przez pracodawcę oraz umożliwiać kontakt z psychologiem lub innym wsparciem dla osób zmagających się ze stresem wojennym – mówi Magdalena Zwolińska.

Kinga Ciosk zaznacza, że wsparciem dla menedżerów może być także współpraca z psychologami biznesu. To inwestycja w odporność całej organizacji.

Etap 5 Dodatkowe zabezpieczenia

W sytuacjach kryzysowych szczególnego znaczenia nabiera ochrona danych osobowych i tajemnicy przedsiębiorstwa. Pracodawcy powinni zadbać w związku z tym o szyfrowanie i bezpieczne backupy danych, ograniczenie dostępu do systemów wyłącznie do uprawnionych osób czy procedury reagowania na incydenty cyberbezpieczeństwa.

– Konieczne jest też uregulowanie zasad korzystania z prywatnych urządzeń do celów służbowych – wskazuje Agata Majewska. Chodzi o wdrożenie BYOD (Bring Your Own Device), czyli praktyki polegającej na umożliwieniu pracownikom korzystania z ich osobistych urządzeń, takich jak laptopy, smartfony czy tablety, do celów służbowych.

– Niezbędne jest też przeszkolenie pracowników, by wyostrzyć ich czujność na zachowania, które mogą mieć na celu zainfekowanie infrastruktury IT, wyłudzenie danych firmowych itp. – zauważa Agata Majewska.

Doktor Katarzyna Kalata zaznacza, że podstawą bezpieczeństwa są regularne kopie zapasowe danych, przechowywane w bezpiecznym miejscu (np. w chmurze). Równie ważna jest ochrona systemów IT – aktualne oprogramowanie, antywirusy, szyfrowanie ważnych danych i bezpieczny zdalny dostęp (VPN). Trzeba także mieć plan odzyskiwania danych po awarii oraz zabezpieczenia fizyczne (awaryjne zasilanie, ochrona dokumentów).

Magdalena Zwolińska przypomina, że w sytuacjach wyjątkowych, takich jak wojna, regulacje dotyczące ochrony danych osobowych, w tym przepisy RODO, mogą przewidywać wyjątki, które pozwalają na przetwarzanie danych osobowych bez standardowych ograniczeń. Przykład może stanowić brak konieczności uzyskania pełnej zgody pracowników na przetwarzanie danych osobowych ze względu na pilne działania ratunkowe. Jednakże ograniczenia muszą się odbywać z zachowaniem zasady minimalizacji, tj. zbierane powinny być tylko te dane, które są niezbędne do osiągnięcia celu oraz z zachowaniem zasady proporcjonalności.

Przypomina jednocześnie o zabezpieczeniu sprzętu i oprogramowania do pracy zdalnej, przy wykorzystaniu VPN i szyfrowania. Namawia do regularnego wykonywania kopii zapasowych danych i testowania procedur odtwarzania.

– Warto przypominać pracownikom podstawowe zasady korzystania ze sprzętu służbowego i systemów firmowych. To drobiazgi, jak dbanie o hasła, logowanie się tylko na firmowych urządzeniach czy zgłaszanie wątpliwości do działu IT. Takie przypomnienia realnie zmniejszają ryzyko incydentów. Są też jasnym sygnałem, że pracownicy są partnerami w trosce o wspólne bezpieczeństwo – informuje Robert Stępień.

Etap 6 Zarządzanie płynnością finansową i zasobami

Magdalena Zwolińska wspomina jeszcze o przygotowaniu planu finansowego zabezpieczającego przedsiębiorstwo przed skutkami kryzysu (np. redukcja kosztów, dywersyfikacja dostawców). Zachęca do zapewnienia środków na utrzymanie wypłat dla pracowników i podstawowej działalności.

– W przypadku całkowitej niewypłacalności pracodawcy, na przykład gdy ogłosi on upadłość lub toczy się wobec niego postępowanie restrukturyzacyjne, można ubiegać się o wypłatę wynagrodzenia z Funduszu Gwarantowanych Świadczeń Pracowniczych (FGŚP). Fundusz ten pokrywa m.in. wynagrodzenie za pracę, ekwiwalent za urlop oraz odprawy, ale istnieją ograniczenia czasowe dotyczące okresu, za który są wypłaty. Wniosek do FGŚP składa się przez syndyka, likwidatora lub bezpośrednio w wojewódzkim urzędzie pracy, dołączając dokumenty potwierdzające niewypłacalność pracodawcy i niezapłacone wynagrodzenia – przypomina. Podkreśla jednak, że pracodawca nie może usprawiedliwiać okolicznością wojny braku wypłacania pensji pracownikom.