30 lat WARDYŃSKI + WSPÓLNICY

POLITYKA NA WYPADEK DAWN RAID

dlaczego warto rozważyć jej wdrożenie?

2020

Czym jest dawn raid?

Dawn raid to niezapowiedziana kontrola pomieszczeń należących do przedsiębiorstwa, zwykle w ramach dochodzenia prowadzonego przez organ regulacyjny lub wykonawczy.

Każde przedsiębiorstwo, bez względu na rozmiar, może zostać poddane kontroli organów państwowych. Niezapowiedziane kontrole są zwykle wszczynane w wyniku skargi (klienta, kontrahenta itd.), anonimowego zgłoszenia lub wniosku przedsiębiorcy o odstąpienie od wymierzenia kary pieniężnej (tzw. wniosek leniency). Kontrole mogą też być wszczynane przez organy z urzędu.

W Polsce wiele organów ma prawo przeprowadzić przeszukania pomieszczeń służbowych. To, czy i jaki organ skontroluje pomieszczania należące do przedsiębiorcy, zależy w dużym stopniu od rodzaju działalności prowadzonej przez tego przedsiębiorcę. Większość przedsiębiorstw może być kontrolowana przez organy podatkowe, ZUS, Inspekcję Pracy, Urząd Ochrony Danych Osobowych oraz Urząd Ochrony Konkurencji i Konsumentów. Ci przedsiębiorcy, którzy prowadzą działalność w obszarach regulowanych, mogą podlegać kontroli także innych wyspecjalizowanych organów (np. Państwowej Inspekcji Sanitarnej, Inspekcji Handlowej, Inspekcji Ochrony Środowiska, Straży Granicznej czy Krajowej Administracji Skarbowej).

Uprawnienia kontrolne organów są różne. Zależą też one od zakresu kontroli określonego w nakazie lub postanowieniu wydanym przez organ. Przy najszerszym możliwym zakresie uprawnień funkcjonariusze mogą wejść do pomieszczeń, poszukiwać dokumentów oraz plików elektronicznych, zajmować te pliki i dokumenty, a także zająć sprzęt (np. komputery lub nośniki pamięci). Mogą także przesłuchiwać pracowników, a nawet zamknąć i zapieczętować pomieszczenia.

Niezapowiedziana kontrola powoduje zatem poważne perturbacje dla biznesu. Należy się do niej odpowiednio przygotować, aby zmniejszyć ryzyko popełnienia błędów i ograniczyć niedogodności.

Czym jest polityka na wypadek dawn raid?

Polityka na wypadek dawn raid to prosta i przejrzysta procedura postępowania dla personelu, w szczególności tych osób, które w pierwszej kolejności będą miały styczność z kontrolerami (pracownicy recepcji, ochrona, dział IT, prawnicy wewnętrzni).

Oczywiście nie ma jednej uniwersalnej polityki na wypadek dawn raid. Trzeba ją przygotować przy uwzględnieniu indywidualnych cech danej organizacji. Pewne elementy wspólne powinny jednak pojawić się w każdej polityce.

1. Rozpoczęcie przeszukania. Pierwszy kontakt z funkcjonariuszami

Pracownicy recepcji i ochrony muszą otrzymać jasne instrukcje, co mają zrobić, gdy zwrócą się do nich funkcjonariusze organu kotrolującego. Zazwyczaj polityka przewiduje, że funkcjonariuszy należy wpuścić na teren przedsiębiorstwa, a pracownicy recepcji powinni uprzejmie poprosić ich, aby poczekali na osoby mające odpowiednie uprawnienia do dalszego postępowania.

2. Weryfikacja uprawnień

Polityka powinna wskazywać osoby odpowiedzialne za weryfikację nakazu i sprawdzenie legitymacji służbowej funkcjonariuszy.

3. Poinformowanie kadry kierowniczej o kontroli

Pracownicy recepcji i ochrony muszą wiedzieć, że o kontroli należy niezwłocznie poinformować odpowiednich członków kadry kierowniczej. W tym celu powinni dysponować aktualnymi danymi kontaktowymi, a także zdawać sobie sprawę, że nie wystarczy jeden telefon – jeśli nie uda im się skontaktować z odpowiednią osobą za pierwszym razem, kontakt należy ponawiać aż do skutku. Polityka może precyzować także kolejność kontaktu i środki komunikacji.

4. Utworzenie zespołu interwencyjnego

Polityka określa zwykle, kto powinien wejść w skład zespołu interwencyjnego na wypadek dawn raid. Najczęściej będą to członkowie kadry kierowniczej, prawnicy wewnętrzni, pracownicy działu IT i prawnicy zewnętrzni. Oczywiście zazwyczaj nie wszyscy członkowie zespołu interwencyjnego będą na miejscu i mogą potrzebować czasu, aby dotrzeć do miejsca kontroli. Dlatego ważne jest, aby w każdym miejscu, w którym przedsiębiorstwo prowadzi swoją działalność, był zawsze obecny koordynator ds. dawn raid. Powinien on towarzyszyć funkcjonariuszom do czasu przyjazdu zespołu interwencyjnego.

5. IT

Zdecydowana większość dokumentów jest obecnie przechowywana wyłącznie w formie elektronicznej. Dlatego należy sprawdzić, którzy pracownicy działu IT dysponują odpowiednią wiedzą i uprawnieniami, aby skutecznie wspierać spółkę w razie kontroli. Jeśli pracują oni poza siedzibą firmy, należy upewnić się, że odpowiednie osoby posiadają ich dane kontaktowe. Właściwi członkowie zespołu IT powinni zostać niezwłocznie poinformowani o przeszukaniu. Ich pomoc może być bowiem niezbędna przy przeszukiwaniu plików elektronicznych. Informatycy powinni także zabezpieczyć kopie dokumentów elektronicznych. Na czas trwania kontroli wszystkie rutynowe procedury niszczenia dokumentów powinny zostać zawieszone.

6. Zarządzanie personelem

Polityka powinna wskazywać na konieczność poinformowania pracowników o kontroli. Pracownicy nie mogą ukrywać ani niszczyć żadnych dokumentów czy plików elektronicznych. Zabronione jest uzgadnianie zeznań czy wprowadzanie funkcjonariuszy w błąd. Należy poinstruować pracowników, aby współpracowali z funkcjonariuszami, ale nie przekazywali im samodzielnie żadnych materiałów. Pracownicy powinni znać swoje prawa i wiedzieć, czy i kiedy mogą zachować milczenie. Powinni również wiedzieć, czy mogą poprosić o asystę prawnika. Należy koniecznie poinstruować wszystkich członków personelu, aby nie podpisywali żadnych protokołów ani oświadczeń, które nie odzwierciedlają w pełni informacji udzielonych przez nich funkcjonariuszom.

7. Kontrola działań funkcjonariuszy

Jeśli to możliwe, każdemu funkcjonariuszowi powinien towarzyszyć „cień" – członek zespołu lub zewnętrzny prawnik, którego zadaniem jest dopilnowanie, aby funkcjonariusze nie przekraczali swoich uprawnień. Zazwyczaj taka osoba rejestruje wszystkie dokumenty przeglądane przez funkcjonariuszy, wszystkie pytania, które zostały przez nich zadane oraz wszystkich pracowników, którzy byli przesłuchiwani. Te osoby powinny także upewnić się, że funkcjonariusze obchodzą się we właściwy sposób z materiałami wrażliwymi.

Procedura na wypadek niezapowiedzianej kontroli może wykraczać poza proste instrukcje dotyczące sposobu działania na wypadek kontroli. Może przykładowo systematyzować procedury dotyczące sposobu przechowywania i kopiowania dokumentów oraz plików elektronicznych. Dotyczy to w szczególności dokumentów objętych tajemnicami zawodowymi. Powinny być one wyraźnie oznakowane i przechowywane w jednym miejscu.

Wszechstronna polityka na wypadek kontroli powinna obejmować kwestie związane z tworzeniem zapasowych kopii dokumentów i danych. Jeżeli inspektorzy prowadzący przeszukanie skonfiskują twarde dyski, przedsiębiorstwo musi mieć zabezpieczone dane, tak aby po zakończeniu przeszukania mogło niezwłocznie wznowić działalność.

Oczywiście lista problemów, które mogą być uregulowane w polityce, jest otwarta i zależy od rodzaju działalności prowadzonej przez przedsiębiorstwo.

Czy sama polityka wystarczy?

Odpowiedź na to pytanie jest oczywista – sam fakt istnienia polityki nie wystarczy. Musi być ona jeszcze dobrze znana wewnątrz organizacji, w szczególności osobom, które są na „pierwszej linii" (pracownicy recepcji, ochrona, dział IT, prawnicy wewnętrzni).

Musi też być regularnie aktualizowana. Przestarzała polityka znana garstce osób w firmie nie będzie spełniała swojego celu, a nawet może być szkodliwa.

Dlatego należy upewnić się, że wszyscy pracownicy zapoznali się z polityką, a najlepiej, że przeszli również odpowiednie szkolenia. Jednak nawet najlepsze szkolenie, prowadzone w komfortowych warunkach sali konferencyjnej, nie zastąpi możliwości przećwiczenia procedury w praktyce. Próbna kontrola to doskonała metoda na przetestowanie gotowości przedsiębiorstwa do kontroli.

Niemniej nawet najlepsza polityka i przeszkolony personel mogą nie wystarczyć. Obecność funkcjonariuszy w firmie zwykle powoduje stres. Co więcej, jest bardzo prawdopodobne, że w czasie kontroli pojawi się wiele kwestii, na które nie ma łatwej odpowiedzi. Czy funkcjonariuszom należy zapewnić dostęp do zaszyfrowanych dokumentów? Czy trzeba udostępniać pliki przechowywane w chmurze na serwerach w obcej jurysdykcji?

Dlatego warto zapewnić spółce możliwość kontaktu z zewnętrznymi prawnikami mającymi doświadczenie w zakresie dawn raid, a także odpowiednich typów postępowań. Należy pamiętać, że kontrole organów państwowych są bardzo często prowadzone poza standardowymi godzinami pracy (np. w godzinach wczesnoporannych). Dobrze jest zatem znaleźć takiego doradcę prawnego, który będzie dostępny 24/7.

Zespół

Łukasz Lasek
prawo karne

Michał Nowacki
podatki

Antoni Bolecki
ochrona konkurencji

Katarzyna Żukowska
dane osobowe

Szymon Kubiak
prawo pracy

Wardyński i Wspólnicy
Al. Ujazdowskie 10, 00-478 Warszawa

Tel.: 22 437 82 00, 22 537 82 00
Faks: 22 437 82 01, 22 537 82 01
E-mail: warsaw@wardynski.com.pl