Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.103.2024
Warszawa, 23 września 2024 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 27 sierpnia br. Posła na Sejm RP Pana Jana Warzechy w sprawie alarmującego stanu bezpieczeństwa danych osobowych w sektorze małych i średnich przedsiębiorstw w Polsce (interpelacja nr 4452)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytanie.

Ad 1) Czy Ministerstwo planuje przeprowadzić edukację przedsiębiorców z sektora MŚP albo wprowadzić regulacje lub programy wsparcia mające na celu poprawę stanu bezpieczeństwa danych pracowników?

Polskie firmy charakteryzują się niską intensywnością cyfrową (w 2023 r. ponad trzy czwarte polskich przedsiębiorstw została zaliczona do grupy o bardzo niskiej lub niskiej intensywności cyfrowej), a 1/3 polskich firm nie wykorzystuje żadnych narzędzi cyfrowych i jest niezainteresowana ucyfrowieniem swojej działalności[1]. Konsekwencją tego stanu rzeczy jest niska świadomość konieczności dbania o cyberbezpieczeństwo firmy - 90% włamań to phishing. Konieczne jest więc budowanie świadomości zagrożeń, kompetencji cyfrowych i wsparcie we wdrożeniu zabezpieczeń niezbędnych w danej firmie, w ścisłym powiązaniu z jej profilem działalności i stosowanymi rozwiązaniami.

W związku z powyższym, jednym z działań, wpisujących się w Plan Droga do Cyfrowej Dekady 2030, był realizowany w partnerstwie Ministerstwa Rozwoju i Technologii (MRiT) – Ministerstwa Cyfryzacji (MC) oraz Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK-PIB), pilotażowy program pn. „Firma Bezpieczna Cyfrowo". Program Firma Bezpieczna Cyfrowo to program edukacji i certyfikacji cyberbezpieczeństwa dla małych i średnich przedsiębiorstw, którego głównym celem jest podnoszenie świadomości cyfrowej i cyberbezpieczeństwa wśród MŚP, a także upowszechnienie i wdrożenie standardu cyberbezpieczeństwa dla firm w Polsce.

W ramach tego Programu zdefiniowano trzy podstawowe cele:

1) rozwój kompetencji cyfrowych wśród polskich przedsiębiorców, ze szczególnym uwzględnieniem cyberbezpieczeństwa;
2) podniesienie poziomu bezpieczeństwa MŚP oraz stabilności obrotu gospodarczego w Polsce;
3) upowszechnienie i wdrożenie nowego standardu cyberbezpieczeństwa w firmach.

Program Firma Bezpieczna Cyfrowo składa się z dwóch komponentów – edukacyjnego i certyfikacyjnego.

Program Firma Bezpieczna Cyfrowo, jako program kompleksowy edukacji i certyfikacji w obszarze cyberbezpieczeństwa, realizowany jest w trzech etapach (z perspektywy przedsiębiorcy):

1) (auto)diagnoza – weryfikacja stanu cyberbezpieczeństwa i umiejętności cyfrowych firmy poprzez rozbudowaną, wariantową ankietę udostępnioną online pod adresem https://firmabezpiecznacyfrowo.gov.pl);

[1] Społeczeństwo informacyjne w Polsce w 2023 r., Główny Urząd Statystyczny 2023 r., str. 109

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

2) doskonalenie w obszarze bezpieczeństwa cyfrowego i usług cyfrowych – wspieraną przez spersonalizowany raportu i rozbudowany poradnik – etap w którym przedsiębiorca dokonuje adaptacji i modernizacji oraz wprowadza zabezpieczenia w swojej firmie;
3) weryfikacja – etap w którym następuję ocena (przez niezależny podmiot) stanu dojrzałości procesu organizacji zabezpieczeń teleinformatycznych w przedsiębiorstwie tj. ocenę i wydanie certyfikatu przez Jednostkę Certyfikującą NASK-PIB w ramach Programu Certyfikacji „Firma Bezpieczna Cyfrowo"; przedsiębiorca może zdecydować o realizacji pierwszego, dwóch lub wszystkich etapów.

Aktualnie, Ministerstwo Rozwoju i Technologii wspólnie z NASK-PIB rozpoczyna - w celu kontynuacji i rozwinięcia Programu Firma Bezpieczna Cyfrowo - dwa projekty związane ze zwiększeniem cyberodporności małych i średnich przedsiębiorstw poprzez udostępnienie nowych, cyfrowych usług i funkcji wspierających przedsiębiorców w podniesieniu jakości usług cyfrowych i poziomu cyberbezpieczeństwa, a także w dostosowaniu ich działań do wymogów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2) oraz rozporządzenia unijnego Cyber Resilience Act (CRA), jak również innych aktów prawnych w zależności od właściwości.

Pierwszy z nich realizowany jest ze środków Krajowego Planu Odbudowy i Zwiększania Odporności – pod nazwą „Zwiększenie dojrzałości cyfrowej i cyberbezpieczeństwa firm poprzez udostępnienie usług cyfrowych na Biznes.gov.pl", i dotyczy w jednej z części kontynuacji i rozszerzenia pilotażowego Programu Firma Bezpieczna Cyfrowo. W ramach projektu rezultaty pilotażu zostaną zaimplementowane w rozszerzonej wersji do systemu Biznes.gov.pl poprzez m.in. stworzenie nowej usługi analitycznej dot. dojrzałości cyfrowej (analiza luk dojrzałości cyfrowej i poziomu cyberbezpieczeństwa) - ukierunkowanej na diagnozę dojrzałości i rekomendacje doskonalenia w zakresie cyberbezpieczeństwa i wdrożenia usług cyfrowych. W rezultacie przedsiębiorcy znajdą w jednym miejscu, tj. na portalu biznes.gov.pl, informacje o zmianach w przepisach, ankietę do samooceny oraz poradnik opisujący działania, które firma musi wykonać, aby zapewnić zrealizować zamierzone cele dojrzałości cyfrowej i cyberbezpieczeństwa.

W ramach kolejnego projektu realizowanego ze środków pozyskanych w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027, pod nazwą „Kampania edukacyjno-informacyjna dla przedsiębiorców, upowszechniająca korzyści płynące z technologii cyfrowych", zostaną przeprowadzone działania mające na celu wspieranie małych i średnich przedsiębiorstw w zakresie cyberbezpieczeństwa. Celem kampanii edukacyjno-informacyjnej będzie podniesienie powszechnej świadomości o korzyściach płynących z technologii cyfrowych wśród przedsiębiorców i ich pracowników, w szczególności w zakresie e-usług publicznych, cyberbezpieczeństwa, a także w obszarze wykorzystania technologii cyfrowych. Zakłada się realizację 3 kampanii edukacyjno-informacyjnych, w trzech obszarach tematycznych:

1) e-usługi publiczne;
2) cyberbezpieczeństwo;
3) wykorzystanie technologii cyfrowych.

Warto podkreślić, że w sektorze małych i średnich przedsiębiorstw zatrudnionych jest dziś 11,5 mln pracowników, do których planuje się kierować komunikację w ramach opisanej kampanii informacyjno-promocyjnej. Pracownicy są nieodłączną grupą przedsiębiorstwa, a co za tym idzie, mają wysoki wpływ na jego funkcjonowanie. To również od ich kompetencji i wiedzy zależy poziom korzystania z technologii cyfrowych, sposób realizacji spraw w administracji lub higiena pracy w kontekście cyberzagrożeń.

Za realizację obu wymienionych wyżej projektów odpowiada Ministerstwo Rozwoju i Technologii, a wsparcia merytorycznego udziela partner merytoryczny NASK-PIB.

Co do regulacji mających na celu poprawę stanu bezpieczeństwa danych pracowników MŚP, podstawową regulacją dotyczącą ochrony danych osobowych jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietna 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwane dalej „RODO". Przepisy te nakładają na administratorów danych osobowych oraz podmiotów przetwarzających zapewnienie integralności i poufności danych osobowych. Szczególnie istotne są tutaj przepisy art. 32 RODO i art. 28 RODO zgodnie z którymi administrator danych osobowych oraz podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne mające zapewnić stopień bezpieczeństwa danych osobowych odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych. Przepisy te stosuje się bez względu na wielkość administratora danych osobowych czy podmiotu przetwarzającego. RODO wprowadziło administracyjne kary pieniężne za niestosowanie obowiązków z zakresu ochrony danych osobowych. Kwestie proceduralne zostały unormowane w ustawie o ochronie danych osobowych[2]. Przepisy obrosły już praktyką administracyjną Prezesa Urzędu Ochrony Danych Osobowych oraz orzecznictwem sądowym, zarówno tym krajowym jak i europejskim. Przepisy te są wystarczające do zapewnienia poufności danych osobowych i nie wymagają zmiany ani uzupełnienia przez przepisy krajowe. Odrębną kwestią jest sprawa ich faktycznej stosowalności przez administratorów danych osobowych czy podmioty przetwarzające. Tak jak wyżej wskazano są wprowadzone sankcje administracyjne za brak stosowania środków technicznych i organizacyjnych zapewniających poufność danych osobowych. Prezes Urzędu Ochrony Danych Osobowych ma także uprawnienia do prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych.

Przepisy projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) wprowadzają wymóg wdrożenia systemu zarządzania bezpieczeństwem informacji przez podmioty kluczowe i podmioty ważne w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80). Obowiązki te dodatkowo wzmocnią ochronę danych osobowych pracowników podmiotów kluczowych i podmiotów ważnych oraz pracowników podmiotów, którym podmioty kluczowe i podmioty ważne świadczą usługi, np. usługi z zakresu zarządzania usługami ICT (managed services providers). Wraz z wejściem w życie tych przepisów prowadzone będą działania informacyjne o wprowadzanych zmianach, kierowane do poszczególnych grup interesariuszy, w tym również do przedsiębiorców.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

[2] ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 poz. 1781)

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa