Kontakt dla mediów:
Luiza Nowicka, PARP
e-mail: luiza_nowicka@parp.gov.pl
tel.: 880 524 959

Informacja prasowa
Warszawa, 30.03.2023 r.

Cyberbezpieczeństwo w firmie. Jakie narzędzia wesprą ochronę danych?

Cyfrowe zagrożenie dla bezpieczeństwa danych jest jednym z największych współczesnych ryzyk dla biznesu. Nic dziwnego, skoro aż 60% małych firm, które stały się ofiarami cyberataku, upada w ciągu kolejnych sześciu miesięcy[1]. W dzisiejszym cyfrowym świecie wdrożenie odpowiednich zabezpieczeń jest już koniecznością. Jakie narzędzia mają do dyspozycji polscy przedsiębiorcy?

Na jednym z webinarów, realizowanych w ramach cyklu „Idea Rozwoju Twojego Biznesu" przez Polską Agencję Rozwoju Przedsiębiorczości (PARP) w 2021 r., Marek Ostafil z Fundacji Platforma Przemysłu Przyszłości przytoczył alarmujące dane w zakresie cyberbezpieczeństwa w Polsce[2]. Ponad rok temu aż 70% badanych przedsiębiorstw doświadczyło przynajmniej jednego cyberataku. W 2019 r. 54% polskich firm padło ofiarą przestępstw cybernetycznych, a 44% biznesów poniosło straty finansowe na ich skutek. Pierwsze trzy miesiące pandemii, wiążące się z przejściem na zdalny tryb pracy, przyniosły wzrost liczby cyberataków o ok. 500%. A to tylko pojedyncze informacje stanowiące część obrazu, w którym właściwa ochrona danych staje się jednym z większych współczesnych wyzwań. Czym jednak jest cyberbezpieczeństwo?

Cyberbezpieczeństwo w pigułce

ICT (z ang. *information and communication technologies*), czyli technologie informacyjno-telekomunikacyjne, teleinformatyczne lub techniki informacyjne, to wszystkie technologie przetwarzające, gromadzące i przesyłające informacje w formie elektronicznej.

Cyberbezpieczeństwo definiuje się jako całokształt działań podejmowanych w celu zminimalizowania ryzyk grożących ICT i funkcjonowaniu w cyberprzestrzeni (świecie wirtualnym). Obejmują one zapewnienie bezpieczeństwa procesów, działania profilaktyczne, takie jak zapobieganie cyberincydentom i budowanie świadomości w zakresie właściwych zachowań w sieci, a także wyposażenie w odpowiednie technologie i rozwiązania, gwarantujące ochronę danych.

[1] https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html
[2] https://www.parp.gov.pl/images/sites/IdeaRozwojuBiznesu/Marek_Ostafil_-_Cyberbezpieczestwo_-_712_PARP.pdf

Każdy przedsiębiorca, chcący dbać o cyberbezpieczeństwo, powinien zdefiniować: CO i JAK należy chronić przed JAKIMI zagrożeniami. Obszarami, które zawsze będą wymagać zabezpieczenia, są: UŻYTKOWNIK, URZĄDZENIA oraz DANE.

Skuteczna ochrona przed cyberatakami wymaga wypracowania przez firmy odpowiednich kryteriów, zasad i procesów organizacyjnych.

Stan cyberbezpieczeństwa w Polsce

Jak czytamy w „Raporcie o stanie sektora małych i średnich przedsiębiorstw w Polsce" Polskiej Agencji Rozwoju Przedsiębiorczości z 2022 r., firmy mają do wyboru wiele środków służących zapewnieniu bezpieczeństwa lub przynajmniej minimalizowaniu ryzyka wystąpienia incydentów ICT, które mogą mieć destrukcyjny wpływ na ich działalność.

Oprócz nich bardzo ważny jest czynnik ludzki, dlatego przedsiębiorstwa coraz częściej mają sformalizowaną strategię bezpieczeństwa teleinformatycznego i przykładają coraz większą wagę do odpowiedniego wyszkolenia kadr w tym obszarze.

Zgodnie ze wspomnianym opracowaniem w 2021 r. odsetek przedsiębiorstw stosujących jakiekolwiek środki bezpieczeństwa ICT wyniósł 95,3%. Wykorzystywano je przede wszystkim w dużych przedsiębiorstwach (99,9%).

Najczęściej stosowanymi środkami bezpieczeństwa ICT w Polsce były: bieżąca aktualizacja oprogramowania (82,5%) oraz uwierzytelnianie silnym hasłem (79,2%). Do mniej popularnych działań należało wykonywanie zapasowych kopii danych i przekazywanie ich do innych lokalizacji (61,4%). Najrzadziej korzystano z identyfikacji i uwierzytelniania metodami biometrycznymi (8,1%). W 2021 r. 27,9% przedsiębiorstw przeprowadziło audyt bezpieczeństwa systemu informacyjnego firmy. Z tej możliwości najczęściej korzystały podmioty duże (73,7%), a najrzadziej małe (22,8%).

Ustawowe bezpieczeństwo polskiej sieci

W Polsce o bezpieczeństwo danych cyfrowych dba NASK, państwowy instytut badawczy, nadzorowany przez Kancelarię Prezesa Rady Ministrów. Do jego głównych zadań należą działania związane z zapewnieniem bezpieczeństwa internetu, czyli cyberbezpieczeństwa i ochrony użytkowników. NASK na bieżąco reaguje na zdarzenia naruszające bezpieczeństwo sieci w Polsce.

Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa NASK został wskazany jako jeden z Zespołów Reagowania na Incydenty Komputerowe, który koordynuje obsługę niebezpiecznych zdarzeń zgłaszanych przez operatorów usług kluczowych, dostawców usług cyfrowych czy samorząd terytorialny. Do NASK incydenty mogą także zgłaszać wszyscy użytkownicy. Instytucja współtworzy zaplecze analityczne oraz badawczo-rozwoje dla krajowego systemu cyberbezpieczeństwa.

Jak mówi **Kamil Mroczka, członek zarządu NASK S.A.:** – Cyfrowa transformacja dotyczy niemal każdej branży i wszystkich sektorów gospodarki – od usług finansowych, przez edukację i służbę zdrowia, po przemysł. Nowe technologie tworzą wiele nowych korzyści, w tym biznesowych, ale

niosą też zagrożenia. Cyberprzestępcy, wykorzystując różne techniki ataków i luki w systemach zabezpieczeń, mogą podważyć reputację organizacji i wyrządzić jej ogromne szkody, także finansowe. Aby pomóc przedsiębiorstwom – publicznym i komercyjnym – chronić się przed zagrożeniami, proponujemy im bogaty pakiet rozwiązań gwarantujących najwyższy możliwy poziom cyberbezpieczeństwa, łącznie z usługami pozwalającymi na ciągły monitoring infrastruktury teleinformatycznej oraz szybką reakcję na incydenty. Produkty oferowane przez NASK S.A. zapewniają bezpieczeństwo w przenikających się sferach IT i OT. Integrujemy zaawansowane usługi bezpieczeństwa teleinformatycznego, dbamy o optymalny dobór konfiguracji wdrażanych rozwiązań oraz zapewniamy wsparcie w utrzymaniu systemów.

Obok NASK funkcjonuje działający w jego strukturach CERT – zespół specjalistów eliminujących zagrożenia w sieciach komputerowych, który walczy z przestępczością internetową.

CERT Polska wykonuje obowiązki ustawowe w zakresie przyjmowania i obsługi zgłoszeń incydentów, analizy zagrożeń i analizy ryzyka oraz ostrzegania. Zadania finansowane są z budżetu państwa. W działalności badawczo-rozwojowej CERT Polska bierze udział w projektach dofinansowanych ze środków krajowych i europejskich. Dzięki temu obsługa incydentów cyfrowych realizowana jest bezpłatnie.

Dotyczą one w szczególności: wyłudzeń w internecie, złośliwego oprogramowania, ataków typu DoS (*Denial of Service*) i DDoS (*Distributed Denial of Service*), włamań i prób włamania.

Programy wsparcia dla przedsiębiorców

Dysponowanie przez firmy odpowiednim zapleczem w zakresie bezpieczeństwa cyfrowego bez wątpienia stało się już tak zwanym *must-have*. W czasach rosnących zagrożeń i cyberprzestępczości bez należytej ochrony danych trudno o pewność i stabilność funkcjonowania współczesnych przedsiębiorstw.

Przedsiębiorcy działający na terenie Polski, chcący usprawnić działanie swoich firm w zakresie cyberbezpieczeństwa, mogą starać się o dofinansowanie na ten cel z poszczególnych konkursów finansowanych z programów: Fundusze Europejskie dla Nowoczesnej Gospodarki (FENG) oraz Fundusze Europejskie dla Polski Wschodniej (FEPW).

Jednym z nich jest trwający właśnie konkurs „**Ścieżka SMART”**, finansowany z Funduszy Europejskich dla Nowoczesnej Gospodarki i wdrażany przez PARP. W ramach tego naboru jednym z dostępnych modułów fakultatywnych jest cyfryzacja, dzięki któremu możliwe jest dofinansowanie transformacji cyfrowej oraz zapewnienia cyberbezpieczeństwa działalności przedsiębiorstwa. Działania zaplanowane w projekcie, w ramach konkursu, muszą prowadzić do wdrożenia innowacji produktowej lub procesowej przynajmniej na poziomie przedsiębiorstwa. Łączna kwota wsparcia przeznaczona na obecny nabór to miliard złotych.

Więcej informacji o wsparciu cyberbezpieczeństwa w ramach „Ścieżki SMART” można znaleźć na stronie PARP.

Kolejnym konkursem wspierającym w tym obszarze jest **„Współfinansowanie działań EDIH”,** finansowane również z FENG. Skierowany do Europejskich Centrów Innowacji Cyfrowych (EDIH), czyli punktów kompleksowej obsługi wspierających mikro, małe i średnie przedsiębiorstwa w zakresie wdrażania najnowszych rozwiązań cyfrowych w działalności biznesowej. Stanowią one element Programu Europa Cyfrowa. Łączny budżet na nabór to aż 245 mln złotych. Celem programu jest zwiększenie konkurencyjności przedsiębiorstw dzięki procesowi transformacji cyfrowej przez usługi oferowane za pośrednictwem Europejskich Hubów Innowacji Cyfrowych, wyznaczonych przez Komisję Europejską. W Polsce jest ich łącznie 10. Wśród nich znajdują się np. Sieć Badawcza Łukasiewicz – Przemysłowy Instytut Automatyki i Pomiarów PIAP, Krakowski Park Technologiczny Sp. z o.o., Łódzka Specjalna Strefa Ekonomiczna S.A., Pomorska Specjalna Strefa Ekonomiczna Sp. z o.o. oraz Gmina Kielce/Kielecki Park Technologiczny. W ramach „Współfinansowania działań EDIH” możliwe jest pozyskanie budżetu na rozbudowę potencjału kadrowego oraz działalność o charakterze informacyjno-promocyjnym, demonstracyjnym, edukacyjno-szkoleniowym, doradczym i wdrożeniowym.

O wsparcie wnioskować mogą instytucje wspierające biznes, instytucje nauki i edukacji oraz przedsiębiorstwa, które po krajowej prekwalifikacji prowadzonej przez Ministerstwo Rozwoju i Technologii, aplikowały i uzyskały grant KE w konkursie europejskim z Programu Europa Cyfrowa. Wnioski będzie można składać do 20 kwietnia 2023 roku.

Więcej o konkursie „Współfinansowanie działań EDIH” można przeczytać na stronie PARP.

Do dyspozycji przedsiębiorców będzie również konkurs **„Automatyzacja i robotyzacja w MŚP”**, realizowany z Funduszy Europejskich dla Polski Wschodniej. W ramach inicjatywy o dofinansowanie będą mogły ubiegać się przedsiębiorstwa z województw: lubelskiego, podkarpackiego, podlaskiego, świętokrzyskiego, warmińsko-mazurskiego, a także części Mazowsza (bez Warszawy i przyległych powiatów). Działaniami objętymi wsparciem będą m.in. przeprowadzenie w firmie audytu procesów produkcyjnych, usługowych i biznesowych oraz wdrożenie rozwiązań zaplanowanych w mapie transformacji cyfrowej, w tym przeszkolenie/przekwalifikowanie pracowników do obsługi nowych procesów. Budżet konkursu na 2023 rok to 100 mln zł. Rozpoczęcie składania wniosków planowane jest na 2 sierpnia br.

Więcej informacji o programie FEPW znajduje się na stronie PARP.