Cyberbezpieczeństwo w samorządzie

Podniesienie poziomu cyberbezpieczeństwa w samorządzie wykorzystując dofinansowanie z Ministerstwa Cyfryzacji

2023

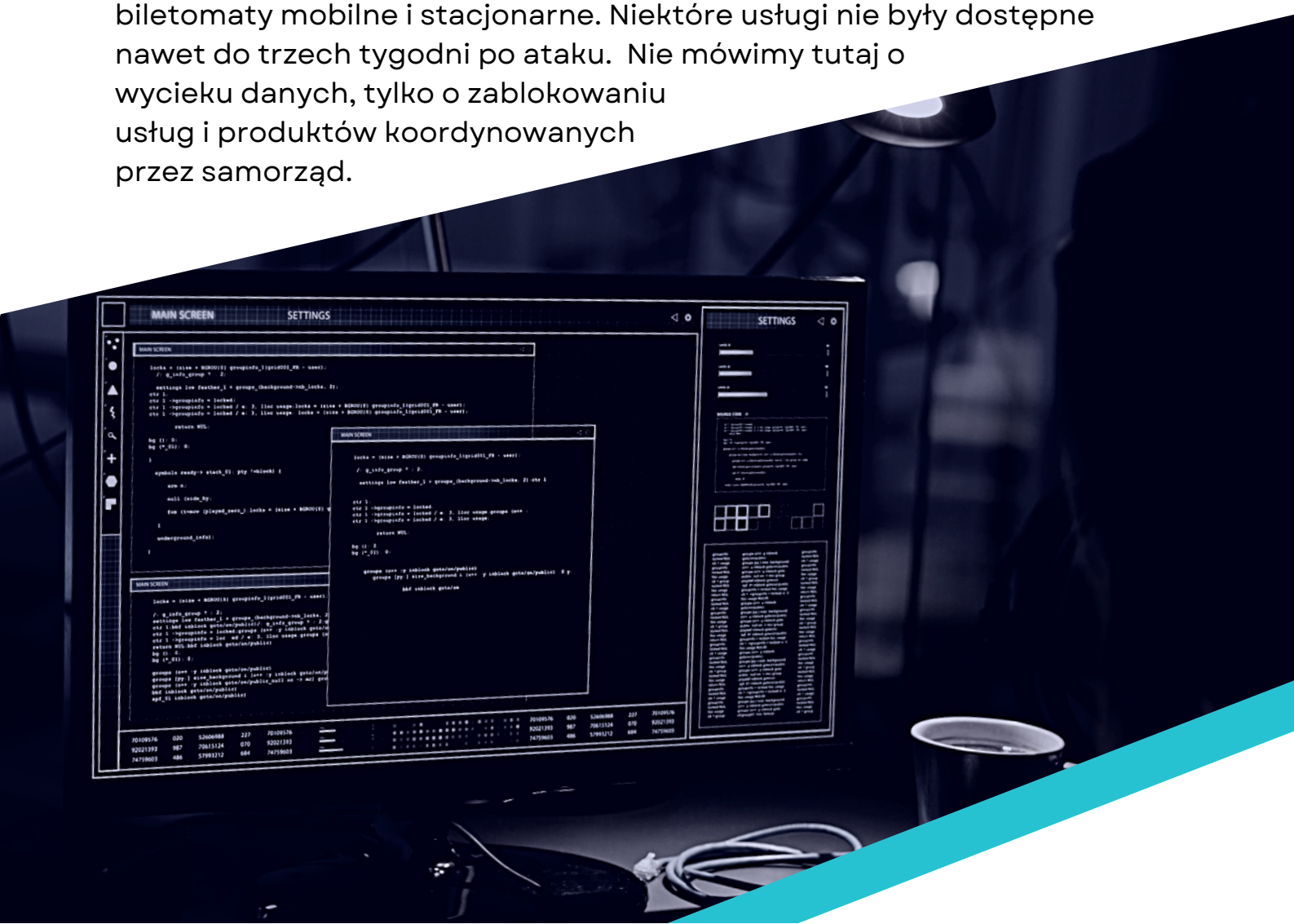
PRZEDSIEBIORCY.PL
SEKCJA BEZPIECZEŃSTWA

Dlaczego warto zadbać o cyberbezpieczeństwo?

Infrastruktura rządowa i samorządowa do 2022 cieszyła się nieznacznym zainteresowaniem cyberprzestępców. Jednak wojna na Ukrainie i Polskie zaangażowanie w pomoc jej obywatelom spowodowały, że nasz kraj jest jednym z głównych celów ataków rosyjskich hackerów. Poniżej przykłady ataków na polskie samorządy:

- atak hackerski na Urząd Miasta Katowic w 2022 r. spowodował wyciek danych osobowych 5 tys. osób w tym pracowników
- atak hackerski na Urząd Miasta Łodzi w 2022 r. spowodował wyciek danych osobowych 2 tys. osób

Ostatni głośny atak hackerski na Zarząd Dróg Transportu i Zieleni w Olsztynie miał miejsce w czerwcu 2023 r. Na skutek ataku nie działała sygnalizacja świetlna, kodowanie miesięcznych biletów, a także biletomaty mobilne i stacjonarne. Niektóre usługi nie były dostępne nawet do trzech tygodni po ataku. Nie mówimy tutaj o wycieku danych, tylko o zablokowaniu usług i produktów koordynowanych przez samorząd.



Pismo wydane przez Kancelarię Prezesa Rady Ministrów

W kwietniu 2023 r. Kancelaria Prezesa Rady Ministrów przesłała do wszystkich podmiotów przyłączonych do węzła krajowego pismo ze wskazaniem jakie aspekty bezpieczeństwa informacji są do poprawy lub wdrożenia od początku. Jak można podnieść poziom cyberbezpieczeństwa:

1. Przede wszystkim Kancelaria wskazała na potrzebę **wdrożenia systemu zarządzania bezpieczeństwem informacji** w oparciu o normę ISO 27001 . Ważne aby system zarządzania obejmował wszystkie informacje, nie tylko dane osobowe.

2. Wprowadzić zasady **zarządzania bezpieczeństwem w relacjach z dostawcami**. Czyli określanić wymogi bezpieczeństwa dla dostawców i zasady ich sprawdzania.

3. Przeprowadzić udokumentowaną **analizę ryzyka** dla bezpieczeństwa informacji, w tym dla systemów informatycznych.

4. **Monitorować** istniejące procedury i stosowane środki zabezpieczajace wraz z określeniem osób odpowiedzialnych i metod prowadzenia monitorowania.

5. Wykonać **przegląd i aktualizację istniejących procedur** dotyczących RODO, a także przeprowadzić cykliczne przeglądy zarządzania bezpieczeństwem informacji.

6. Cyklicznie **zwiększać świadomość** pracowników w zakresie cyberbezpieczeństwa. Nie wystarczy już jedno szkolenie raz na 2 lata.

Dlaczego akurat teraz najlepiej zająć się cyberbezpieczeństwem?

Dofinansowanie na podniesienie poziomu cyberbezpieczeństwa

19 lilpca 2023 r. Ministertwo Cyfryzacji ogłosiło grant "Cyberbezpieczny Samorząd", czyli dofinansowanie dla jednostek samorządu terytorialnego na podniesienie poziomu cyberbezpieczeństwa

Wysokość dofinansowania:

- Gminu w przedziale od 200 000 PLN do 850 000 PLN
- Powiaty do 850 000 PLN
- Województwa do 850 000 PLN

Wnioski o dofinansowanie można składać do 30 listopada. Przy składaniu wniosku należy uzupełnić ankietę dotyczącą aktualnego stanu bezpieczeństwa w jednostce.

Po prawej stronie został wskaznay zakres co jest objęte dofinansowaniem.

WAŻNE - wdrożone rozwiązania należy utrzymać co najmniej przez 2 lata.

Obszar organizacyjny

Wdrożenia ISO 27001, audyty zerowe i audyty certyfikujące,
Przygotowanie dokumentacji związanej z bezpieczeństwem informacji w tym analizy ryzyka i relacji z dostawcami

Kompetencje

Szkolenia dla pracowników
Szkolenia dla kadry zarządzającej
Szkolenia dla działów IT
Testy socjotechniczne

Obszar techniczny

Zakup oprogramowania do SOC i SIEM lub zatrudnienie firmy zewnętrznej
Przeprowadzenie testów penetracyjnych systemów informatycznych
Zakup zewnętrznych konsultacji z ekspertem z cyberbezpieczeństwa

Cyberbezpieczeństwo
Nasze usługi

RODO i KRI

Wdrożenia, przygotowanie dokumentacji, audyty, sprawowanie funkcji Inspektora Ochrony Danych.

ISO 27001

Audyt zerowy, przygotowanie dokumentacji SZBI, wdrożenie dokumentacji w tym analizy ryzyka i relacji z dostawcami, audyt powdrożeniowy, zewnętrzne wsparcie przy dalszym doskonaleniu SZBI.

Szkolenia

Szkolenia dla pracowników i kadry zarządzającej, szkolenia specjalistyczne dla Działów IT. Innowacyjne metody zwiększania świadomości pracowników np. newsletter, quiz.

Zewnętrzny SOC

Bieżące monitorowanie bezpieczeństwa w sieci samorządu, w tym skanowanie podatności, bieżące informowanie o podejrzanych działaniach.

Testy Cyber

Przeprowadzanie testów socjotechnicznych. Przeprowadzanie testów penetracyjnych systemów informatycznych i teleinformatycznych. Przeprowadzanie testów stron internetowych.

Zewnętrzny Pełnomocnik ds. cyberbezpieczeństwa

Wsparcie w napisaniu strategii cyberbezpieczeństwa dla jednostki, punkt kontaktowy w zakresie incydentów cyberbezpieczeństwa, pomoc w zgłoszeniu incydentów do odpowiedniego organu, sprawowanie nadzoru nad reakcją na incydenty, sprawowanie nadzoru nad dokumentacją systemu cyberbezpieczeństwa.

W czym możemy Państwu pomóc?

Przede wszystkim zachęcamy do skorzystania z dofinansowania. Proponujemy współpracę na poniższych zasadach.

01 Uzupełnienie ankiety

Aby złożyć wniosek należy uzupełnić ankietę wskazując aktualny stan cyberbezpieczeństwa w jednostce. Pomożemy uzupełnić ankietę w oparciu o informacje pozyskane podczas konsultacji z pracownikami.

02 Analiza ankiety

Przeanalizujemy wspólnie wyniki ankiety i zaproponujemy działania, które faktycznie zwiększą poziom cyberbezpieczeństwa i będą objęte dofinansowaniem.

03 Przeprowadzenie działań

Przeprowadzenie ustalonych działań. Przykładowa lista: wykonanie audytu zerowego, wdrożenie normy ISO 27001, aktualizacja procedur związanych z RODO, przeprowadzenie testów penetracyjnych.

04 Pomoc przy rozliczeniu

Pomagamy przy rozliczeniu dofinansowania. Jeżeli ministerstwo będzie chciało sprawdzić wdrożone działania, będziemy w tym uczestniczyć.

05 Dalsze wsparcie

Po wdrożeniu wszystkich działań i rozliczeniu projektu służymy konsultacjami i pomocą przy utrzymaniu wdrożonych rozwiązań.

Co samorząd zyska zwiększając poziom cyberbezpieczeństwa?

1. Spełnienie wymagań RODO i KRI
2. Spełnienie części wymagań KSC
3. Realizację rekomendacji wskaznaych w piśmie z Kancelarii Prezesa Rady Ministrów
4. Zadbanie o bezpieczeństwo infrastruktury niezbędnej do zapewnienia ciągłości działania urzędu
5. Zapewnienie większego bezpieczeństwa dla danych osobowych mieszkańców gminy, powiatu czy województwa - czyli danych osobowych wyborców

Kim jesteśmy?

Sekcja Bezpieczeństwa to zespół ekspertów zajmujących się szeroko rozumianym bezpieczeństwem w administracji publicznej i przedsiębiorstwach. Zajmujemy się zarządzaniem bezpieczeństwem cybernetycznym, finansowym, fizycznym, kryzysowym oraz prawnym.

Nasi Liderzy

Mariusz Piętka

Piotr Oleksiak

Agnieszka Kordalewska

Jakub Betka

Mateusz Leszczyński

Zenon Zalewski

Zofia Pruchniak

Radosław Krzypkowski

Pozostałe usługi Sekcji

Sztuka przterwania

Sztuka przeżycia
Plany awaryjnej komunikacji i nawigacji
Zestawy awaryjne
Bezpieczny w domu i w pracy

Bezpieczeństwo fizyczne

Wykonanie wizji lokalnej obiektu, pod kątem weryfikacji zabezpieczeń mechanicznych, elektronicznych i informatycznych, zapoznania się z dokumentacją ochronną, przeprowadzenia wywiadów z osobami odpowiedzialnymi za bezpieczeństwo obiektu, miejsc szczególnie zagrożonych i biorących udział w procesach logistycznych.

Detektywistyka

Doradztwo w zakresie ochrony informacji niejawnych, procedur obronnych, tajemnicy przedsiębiorstwa, zarządzania ryzykiem, zagrożeń terrorystycznych, działań technikami OSINT/HUMINT. Odtwarzanie danych, analiza ataków hackerskich. Badania wariograficzne i antypodsłuchowe.

Bezpieczeństwo finansowe

Ubezpieczenie od ryzyk cybernetycznych.
Ubezpieczenie chroni w szczególności przed skutkami ataków komputerowych (atak hackerski, złośliwe oprogramowanie) oraz następstwami naruszeń danych osobowych.
Ubezpieczenie obejmuje ochroną:

- finansowe skutki wycieku danych elektronicznych,
- koszty dodatkowe i zysk utracony w wyniku ataku komputerowego,
- odpowiedzialność cywilną

Od czego najlepiej zacząć?

Od rozmowy.

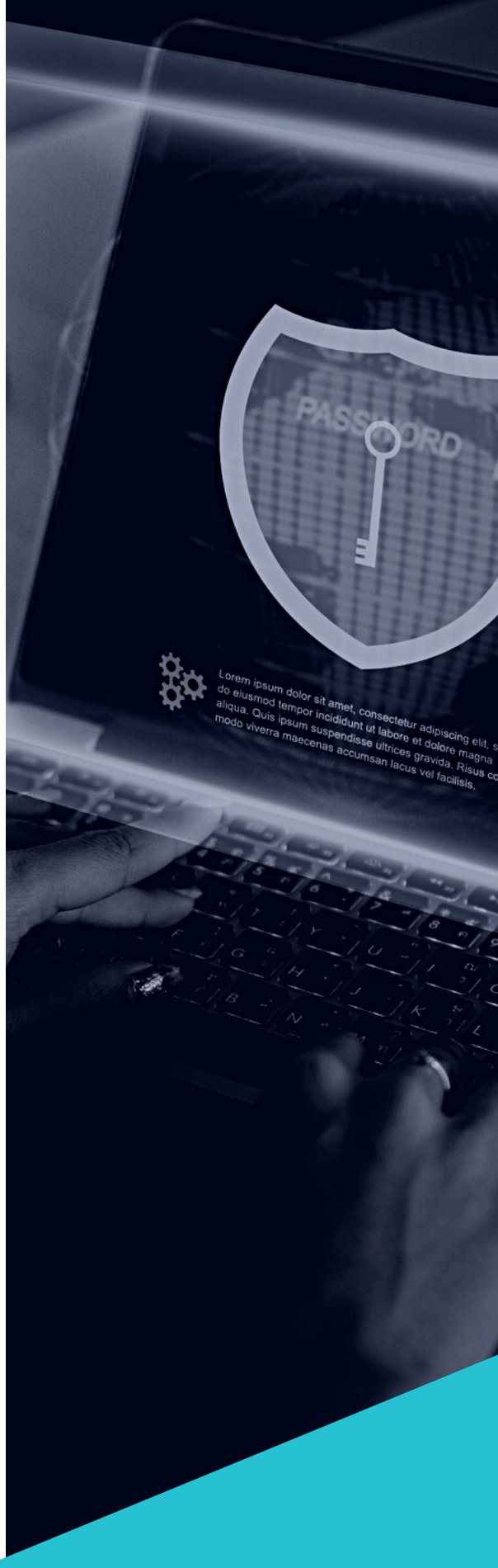
Jeżeli:

- w dalszym ciągu nie wiecie Państwo jak rozpocząć temat cyberbezpieczeństwa w swoim samorządzie;
- oddelegowano temat do Działu IT, ale nie ma pewności czy podołają tej kwestii;
- chcecie Państwo zwiększyć świadomość pracowników w zakresie cyberbezpieczeństwa;
- nie otrzymaliście Państwo informacji w jakiej kwocie urząd może skorzystać z dofinansowania;
- zastanawiacie się Państwo w jaki sposób zwiększyć poziom cyberbezpieczeństwa w samorządzie;
- urząd ma problem z uzupełnieniem ankiety w ramach dofinansowania;
- macie Państwo pytania do Naszej oferty.

Zachęcamy do kontaktu!

Macie Państwo możliwość umówienia się na bezpłatną konsultację telefoniczną, podczas której będziemy mogli odpowiedzieć na Państwa pytania.

PRZEDSIEBIORCY.PL
SEKCJA BEZPIECZEŃSTWA



Zapraszamy do kontaktu

Tel:
722 213 636
792 834 345

E-mail:
sekcjabezpieczenstwa
@przedsiebiorcy.pl