Cyberbezpieczny Samorząd
Nowe możliwości finansowania

https://www.eauditor.eu/cyberbezpieczny-samorzad-cyberbezpieczenstwo-samorzadowych-systemow-informatycznych/

Badanie bezpieczeństwa stron internetowych samorządów, jakie przeprowadzone zostało przez zespół CSIRT NASK w 2020 r. ujawniło **szokujące dane**. W ponad połowie zbadanych witryn odkryto **podatności na ataki**, w tym poważne błędy. Są one coraz częściej zauważane i wykorzystywane przez **cyberprzestępców**. Dowodem na to jest fakt, że w drugiej połowie 2022 r. zarysował się wyraźny trend wzrostowy w liczbie rejestrowanych przez CSIRT NASK zgłoszeń.

Centrum Projektów Polska Cyfrowa we współpracy z Państwowym Instytutem Badawczym NASK rozpoczęło przyjmowanie wniosków w ramach projektu **„Cyberbezpieczny Samorząd”**. Projekt ten skierowany jest do **ponad 2,8 tys. jednostek samorządu terytorialnego**. Gminy, powiaty i województwa mogą uzyskać pieniądze m.in. na **opracowanie, wdrożenie i certyfikację procedur** z zakresu zarządzania bezpieczeństwem informacji, czy też **zakup, wdrożenie i konfigurację systemów, urządzeń i usług** mających na celu podniesienie poziomu cyberbezpieczeństwa.

Realizacja projektu w jednostce samorządu terytorialnego przyczyni się m.in. do:

- wdrożenia lub aktualizacji polityk bezpieczeństwa informacji
- wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie
- wdrożenia mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni

Termin składania wniosków

od **19 lipca** do **14 grudnia** 2023 r.

Wysokość dotacji

od **200 tys.** do nawet **850 tys.** zł

Finansowanie uzależnione od

liczby mieszkańców i **zamożności** jednostki

Do zapewnienia wkładu własnego, którego łączna wysokość dla całego projektu to zaledwie **ok. 4 proc.**, będą zobowiązane tylko najzamożniejsze samorządy. Samorządy będą mogły **rozliczyć** w ramach projektu działania zrealizowane pomiędzy **1 czerwca 2023 r., a 30 czerwca 2026 r.**

Zarządzanie bezpieczeństwem informacji w jednostce obejmuje szeroki zakres działań związanych z opracowaniem i wdrażaniem regulacji, polityk czy procedur. Wymaga także posiadania odpowiedniej infrastruktury IT. **Firma BTC** od ponad 20 lat wspiera jednostki administracji publicznej w zarządzaniu oraz zapewnianiu bezpieczeństwa infrastruktury IT.

Umożliwiają to wdrażane przez nas systemy:

- **eAuditor** - Kompleksowe rozwiązanie do zarządzania, inwentaryzacji, monitorowania i zapewnienia bezpieczeństwa IT. Oprogramowanie eAuditor wspiera kluczowe procesy w organizacji oraz stanowi kompleksowe wsparcie dla działów IT.
- **Hyprovision DLP** - Profesjonalny system do ochrony przed wyciekiem danych, który oferuje szerokie możliwości kontrolowania i blokowania serwerów. Zapobiega także ich utracie oraz pozwala na wykrywanie podejrzanych działań.
- **System Zarządzania Uprawnieniami** - Kompleksowe oprogramowanie automatyzujące procesy nadawania, weryfikacji oraz odbierania uprawnień do systemów IT. Wpływa na zwiększenie bezpieczeństwa IT, dzięki zapewnieniu możliwość bieżącego monitorowania uprawnień.
- **Moduł dla Sygnalistów** - System dedykowany do przyjmowania zgłoszeń o naruszeniach prawa od Sygnalistów, zgodnie z przepisami Dyrektywy Parlamentu Europejskiego i Rady UE. To bezpieczny kanał informujący o nieprawidłowości w organizacjach.
- **eHelpDesk** - Rozwiązanie do zarządzania procesami wsparcia technicznego. System umożliwia nadzorowanie świadczonych usług informatycznych oraz zarządzanie incydentami w celu ograniczania ich negatywnego oddziaływania na biznes.
- **RODOprotektor** - Rozwiązanie do zarządzania danymi osobowymi zgodnie z RODO. Wspiera administratorów danych i inspektorów ochrony danych w realizacji codziennych zadań, umożliwiając nadzór nad upoważnieniami oraz szacowanie potencjalnego zagrożenia.

Dlaczego warto wybrać system eAuditor w ramach Programu Cyberbezpieczny Samorząd?

System eAuditor spełnia wszystkie wymogi dotyczące zapewniania cyberbezpieczeństwa samorządowych systemów informatycznych. W ramach programu „Cyberbezpieczny Samorząd" proponujemy wdrożenie naszych rozwiązań, zwiększających **poziom bezpieczeństwa IT** w podmiotach jednostek samorządu terytorialnego. Nasi Klienci doceniają to, że przekazujemy działom IT kompleksowe rozwiązanie, które już w konfiguracji podstawowej umożliwia: **zapewnienie bezpieczeństwa IT, zarządzanie IT, inwentaryzację IT** oraz **monitorowanie IT.**

wskaźniki bezpieczeństwa
infrastruktury IT (SOC)

bezpieczne zdalne połączenia z komputerami
w sieci lokalnej i za NAT z wykorzystaniem technologii RTC

zdalne i masowe szyfrowanie
partycji systemowych i niesystemowych dla SSD/HDD i USB za pomocą MS BitLocker

monitorowanie uprawnień
MS ACL

Funkcjonalności do zapewnienia bezpieczeństwa IT

polityki bezpieczeństwa DLP

Kiosk Aplikacji
jako metoda bezpiecznego instalowania oprogramowania przez pracowników

sztuczna inteligencja (AI)
w procesie klasyfikowania stron internetowych na podstawie zawartości (treść) strony

Panel Pracownika
jako efektywna metoda informowania i szkolenia pracowników

Wsparcie działań w zakresie cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych)

Wybrane pozycje

Ochrona (OCH)	Działanie	Proponowane rozwiązanie
(OCH.1) Zarządzanie tożsamościami, uwierzytelnianie i kontrola dostępu	W Jednostce wdrożono system zarządzania tożsamościami i uprawnieniami.	SZU - System zarządzania Uprawnieniami
	Funkcjonuje zarządzanie zdalnym dostępem do zasobów Jednostki.	eAuditor, Hyprovision DLP
	Konta użytkowników i ich prawa dostępu do zasobów są przez Jednostkę zarządzane z uwzględnieniem zasady najniższych uprawnień i rozdzielenia obowiązków.	SZU - System zarządzania Uprawnieniami; eAuditor
	Integralność sieci Jednostki jest chroniona (np. przez segmentację).	eAuditor, Hyprovision DLP
	Weryfikacja dostępu do zasobów Jednostki opiera się na wykorzystania uwierzytelniania wieloskładnikowego (MFA).	eAuditor, Hyprovision DLP; SZU - System zarządzania uprawnieniami
(OCH.2) Świadomość i podnoszenie kompetencji	Użytkownicy ze wysokimi uprawnieniami rozumieją swoje role i obowiązki w Jednostce.	eAuditor LMS - System zarządzania szkoleniami
	Kadra kierownicza wyższego szczebla w Jednostce rozumie swoje role i obowiązki.	eAuditor LMS - System zarządzania szkoleniami
	Personel cyberbezpieczeństwa oraz bezpieczeństwa fizycznego w Jednostce rozumie swoje role i obowiązki.	eAuditor LMS - System zarządzania szkoleniami
(OCH.3) Bezpieczeństwo danych	W Jednostce dane w spoczynku są chronione.	Hyprovision DLP
	W Jednostce dane przesyłane są zabezpieczone.	Hyprovision DLP
	Zasoby Jednostki są formalnie zarządzane podczas usuwania, przenoszenia i dysponowania.	Hyprovision DLP
	Utrzymywana jest odpowiednia zdolność Jednostki do zapewnienia dostępności do jej danych.	eAuditor, Hyprovision DLP
	Wdrożono w Jednostce mechanizmy ochrony przed wyciekami danych.	eAuditor, Hyprovision DLP
(OCH.5) Technologia ochronna	Zapisy zdarzeń / logów / inspekcji są określone, dokumentowane, wdrażane i sprawdzane zgodnie z politykami Jednostki.	eAuditor, Hyprovision DLP
	Nośniki wymienne są chronione, a ich stosowanie jest ograniczone zgodnie z politykami Jednostki.	eAuditor, Hyprovision DLP
	Zasada najmniejszej funkcjonalności jest stosowana w Jednostce przy konfiguracji systemów tak, by posiadały one tylko niezbędne możliwości.	eAuditor, Hyprovision DLP

Zdarzenia i Monitoring (CM)	Działanie	Proponowane rozwiązanie
Anomalie i zdarzenia (CM.1)	Wykryte zdarzenia są w Jednostce analizowane w celu wykrycia metody, przebiegu oraz celu ataków.	Hyprovision DLP
	Dane o zdarzeniach są pozyskiwane z wielu źródeł w infrastrukturze IT Jednostki, a następnie są centralnie korelowane i analizowane.	Hyprovision DLP
Ciągłe monitorowanie bezpieczeństwa (CM.2)	Sieć Jednostki jest monitorowana w celu wykrywania potencjalnych zdarzeń cyberbezpieczeństwa.	Hyprovision DLP
	Środowisko fizyczne Jednostki jest monitorowane w celu wykrycia potencjalnych zdarzeń cyberbezpieczeństwa.	eAuditor, Hyprovision DLP
	Aktywność personelu Jednostki jest monitorowana w celu wykrycia potencjalnych zdarzeń związanych z cyberbezpieczeństwem.	eAuditor, Hyprovision DLP
	Złośliwy kod w oprogramowaniu Jednostki jest wykrywany.	eAuditor, Hyprovision DLP
	Nieautoryzowany kod źródłowy oprogramowania Jednostki jest wykrywany (np. ActiveX, JavaScript).	eAuditor, Hyprovision DLP
	Aktywność zewnętrznych dostawców usług dla Jednostki jest monitorowana w celu wykrywania potencjalnych zagrożeń cyberbezpieczeństwa.	eAuditor, Hyprovision DLP
	Prowadzi się w Jednostce ciągłe monitorowanie pod kątem nieautoryzowanego dostępu, połączeń, urządzeń i oprogramowania.	eAuditor, Hyprovision DLP
	Przeprowadza się w Jednostce cykliczne skanowanie podatności.	eAuditor, Hyprovision DLP

Reagowanie (RE)	Działanie	Proponowane rozwiązanie
Planowanie reagowania (RE)	Plan reagowania na incydenty w Jednostce jest realizowany w trakcie trwania incydentu lub po jego wystąpieniu.	Hyprovision DLP
	Personel Jednostki zna swoje role i kolejność operacji, na wypadek konieczności reagowania na incydenty bezpieczeństwa.	eAuditor, Hyprovision DLP
	Incydenty są zgłaszane w Jednostce zgodnie z ustalonymi procedurami.	eHelpdesk
	Informacje o incydentach bezpieczeństwa są udostępniane w Jednostce zgodnie z planami reagowania na incydenty.	eHelpdesk
	Dobrowolna wymiana informacji Jednostki z zewnętrznymi podmiotami jest prowadzona w celu osiągnięcia szerszej świadomości sytuacyjnej w zakresie cyberbezpieczeństwa.	Wszystkie systemy - poprzez API
	Jednostka jest podłączona do systemu S46.	Wszystkie systemy - poprzez API
Obsługa incydentów (OI)	Incydenty są wykrywane, zgłaszane i obsługiwane w obrębie Jednostki.	eAuditor, Hyprovision DLP, eHelpdesk
	Są prowadzone działania naprawcze po wystąpieniu Incydentów.	eAuditor, Hyprovision DLP, eHelpdesk
	Nowe, zidentyfikowane w Jednostce podatności są usuwane lub akceptowane i dokumentowane są ryzyka związane z nimi.	eAuditor, Hyprovision DLP, eHelpdesk
Doskonalenie (DS)	Plany reagowania na incydenty uwzględniają wyciąganie wniosków z wykrytych i obsłużonych incydentów.	eAuditor, Hyprovision DLP, eHelpdesk
	Polityki reagowania na incydenty w Jednostce są aktualizowane.	eAuditor, Hyprovision DLP, eHelpdesk

Funkcje niezbędne do zapewnienia bezpieczeństwa IT podczas pracy zdalnej

Zarządzanie komputerami

- Dashboard – informacja o infrastrukturze IT
- Zdalna instalacja / deinstalacja
- Zdalny pulpit (RDP, RTC, VNC, UVNC)
- Zdalne zarządzanie Intel VPro / AMT
- Zdalna konfiguracja
- Zdalny restart
- Zdalne wykonywanie skryptów CMD (kilkadziesiąt wbudowanych)
- Zdalne wykonywanie skryptów powershell (kilkadziesiąt wbudowanych)
- Wsparcie techniczne

Użytkownicy

- Informacja o użytkownikach online
- Godzina zalogowania, wylogowania
- Monitorowanie pracy (czas aktywności, nieaktywności)
- Monitorowanie uruchamianych aplikacji
- Monitorowanie uruchamianych procesów
- Monitorowanie drukarek i wydruków
- Monitorowanie stron www na podstawie zawartości (machine learning)
- Monitorowanie poczty i załączników poczty wychodzącej
- Zdalne szkolenia pracowników i monitorowanie postępu procesu szkoleniowego

Monitorowanie urządzeń

- Godzina włączenia, wyłączenia, uśpienia
- Lokalizacja komputera po IP (komputer za NATem)
- Podłączane urządzenia zewnętrzne USB
- Monitorowanie i zarządzanie usługami
- Monitorowanie wydajności (RAM, HDD, CPU)
- Monitorowanie dzienników zdarzeń
- Monitorowanie procesów pracownika

Bezpieczeństwo

- Zdalne szyfrowanie dysków (Bitlocker)
- Szyfrowanie BitLocker USB
- Blokowanie nieautoryzowanych urządzeń zewnętrznych USB
- Blokowanie uruchamianych stron wwww
- Blokowanie uruchamianych procesów

Edukacja i komunikacja

- Zdalne szkolenia pracowników
- Definiowanie własnych materiałów szkoleniowych
- Gotowe filmy instruktażowe w zakresie bezpieczeństwa
- Automatyczna komunikacja z użytkownikami – wysyłanie dowolnych treści z potwierdzeniem otrzymania i przeczytania
- Wyświetlanie pilnych komunikatów u użytkowników (Alert)
- Wyświetlanie komunikatów u użytkowników

Chcesz dowiedzieć się więcej?

Wypełnij formularz i umów się na bezpłatną prezentację!

Odwiedź stronę eAuditor.eu