Uchwała Nr 2917/23
Zarządu Powiatu Stargardzkiego
z dnia 6 października 2023 r.

w sprawie złożenia wniosku w ramach konkursu grantowego „Cyberbezpieczny Samorząd"

Na podstawie art. 32 ust.1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz.U. z 2022 r. poz. 1526 ze zm.) uchwala się co następuje:

§1. 1. Postanawia się złożyć wniosek w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa" dotycząca realizacji konkursu grantowego „Cyberbezpieczny Samorząd".

2. Przedmiotem wniosku jest dofinansowanie zakupu sprzętu i oprogramowania komputerowego w celu zwiększenia poziomu cyberbezpieczeństwa Powiatu Stargardzkiego.

§2. Wykonanie uchwały powierza się Dyrektorowi Biura Obsługi Urzędu.

§3. Uchwała wchodzi w życie z dniem podjęcia.

Iwona Wiśniewska – Starosta Stargardzki .....

Łukasz Wilkosz – Wicestarosta .....

Uzasadnienie

W związku z ogłoszonym konkursem „Cyberbezpieczny Samorząd", mającym na celu podniesienie poziomu cyberbezpieczeństwa w jednostce, po dokonaniu kwalifikacji potrzeb, Biuro Obsługi Urzędu proponuje złożyć wniosek o następujące systemy oraz sprzęt informatyczny:

Lp.	Nazwa	Szacunkowy koszt brutto	Koszt utrzymania	Termin realizacji
1.	Klaster serwerowy z macierzą oraz dyskami	469 000,00 zł	-	24 miesięcy od dnia wejścia w życie Umowy o powierzenie Grantu, jednak nie później niż do 30.06.2026 r
2.	Serwer NAS z dyskami	25 000,00 zł	0,00 zł	
3.	Switche zarządzalne – 3 sztuki	23 000,00 zł	4 500,00 zł/rocznie	
4.	Przedłużenie licencji na program antywirusowy	30 000,00 zł	13 200,00 zł/rocznie	
5.	System skanujący pocztę przychodzącą	53 000,00 zł	19 000,00 zł/rocznie	
6.	System EDR	28 000,00 zł	24 000,00 zł/rocznie	
7.	System SIEM	260 000,00 zł	31 000,00 zł/rocznie	
8.	System zarządzania bezpieczeństwem informacji (SZBI)	25 978,00 zł	-	

1. **Security Information and Event Management (SIEM)** to system bezpieczeństwa do monitorowania i analizy, system ten złożony z wielu komponentów, którego celem jest pomoc organizacjom w wykrywaniu wczesnych zagrożeń i łagodzenie skutków ataków. SIEM łączy kilka różnych dyscyplin i narzędzi w ramach jednego spójnego systemu:
   - Log Management (LMS) – narzędzia używane do tradycyjnego zbierania i przechowywania logów;
   - Security Information Management (SIM) – narzędzia lub systemy koncentrujące się na gromadzeniu i zarządzaniu danymi związanymi z bezpieczeństwem z wielu źródeł, takimi jak: zapory sieciowe – firewalle, switche zarządzalne, serwery DNS, routery, antywirusy, system skanujący mailowe wiadomości przychodzące, system edr,
   - Security Event Management (SEM) – systemy oparte na proaktywnym monitorowaniu i analizie, w tym wizualizacji danych, korelacji zdarzeń i alarmowaniu;
   - moduł User Behaviour Analytics (UBA) - lub sztuczna inteligencja - analiza zachowań użytkowników pozwala na tworzenie dynamicznych reguł i uczenie się sieci organizacji na podstawie dostarczonych danych;

   SIEM łączy wszystkie powyższe elementy w jedną platformę, która wie jak automatycznie zbierać i przetwarzać informacje z rozproszonych źródeł, przechowywać je w jednej scentralizowanej lokalizacji, porównywać różne zdarzenia i generować alerty na podstawie tych informacji.

2. **System skanujący pocztę przychodzącą**:
   Podstawowe cechy sytemu:

- skuteczny antyspam – blokuje adresy IP oraz adresy mailowe, z których rozsyłane są wiadomości-śmieci; program antyspamowy korzysta przy tym z ich listy kontaktów, układanej i aktualizowanej przez wyspecjalizowane w tym celu organizacje,
- usuwa złośliwe linki z wiadomości oraz z ich załączników (dokumentów word, excel, pdf) nie zmieniając treści wiadomości i treści złączników,
- ochronę przed szkodliwym oprogramowaniem – system ten wykrywa zagrożenia na poziomie serwera dostawcy usług internetowych (u nas Home.pl i Alfa.tv), dzięki czemu nie trafiają one do skrzynek pocztowych użytkownika, ale są usuwane przed dotarciem do celu,
- nie zakłóca działania protokołu poczty przychodzącej – jego działanie nie jest z żaden sposób odnotowywane przez skrzynki e-mail i nie ma żadnego wpływu na korespondencję z kontrahentami oraz klientami,

3. **Serwer NAS** - (skrót od Network Attached Storage – sieciowa pamięć masowa) to prosty komputer służący do magazynowania i udostępniania dużych ilości danych. Jego głównym komponentem jest dysk twardy. Profesjonalny NAS do szafy serwerowej mieści w sobie kilkadziesiąt pojemnych dysków i ma rozwiązania ułatwiające ich szybką wymianę, tworzenie kopii zapasowych czy zapobieganie skutkom awarii.

4. **Switch zarządzalny** – typ przełącznika, którym można zarządzać przez dedykowany do tego port. Przełączniki dostępne w kilku rodzajach, zarządzanie warstwy L2, L3 i L4. Dodatkowo mogą też łączyć w sobie funkcje oferowane przez switche inteligentne. Tego typu sprzęt najlepiej sprawdza się w bardzo dużych oraz rozległych infrastrukturach sieci Ethernet, gdzie wymagane jest centralne zarządzanie całą siecią.

   Warstwy sieci Internet składają się z czterech warstw:
   - L4 - warstwy aplikacji, zajmującej się reprezentacją danych dla użytkownika oraz ich kodowaniem,
   - L3 - warstwy transportowej, zapewniającej komunikację pomiędzy różnymi urządzeniami w sieci,
   - L2 - internet, zapewniający najlepszą trasę dla przepływu pakietów,
   - L1 - warstwy dostępu do sieci kontrolującej urządzenia fizyczne i media.

5. **SZBI** - System zarządzania bezpieczeństwem informacji (SZBI) to strategia działania, której celem jest zapewnianie właściwej ochrony informacji. Strategia ta ma zapewnić ciągłe doskonalenie podjętych działań i procedur w celu optymalizacji ryzyka związanego z naruszeniem poufności. System bezpieczeństwa informacji ma chronić w taki sposób przed zagrożeniami, żeby zapewnić organizacji:
   - ciągłość prowadzenia działalności
   - zminimalizować straty
   - maksymalizować zwrot nakładów na inwestycje i działania o charakterze biznesowym

   System Zarządzania Bezpieczeństwem Informacji (ISMS - Information Security Management System) zgodny z normą ISO/IEC 27001 uznawany jest za jedno z najlepszych rozwiązań zapewniających zachowanie poufności, integralności i dostępności informacji, których ochrona jest obecnie naturalnym wymogiem naszych czasów.

6. **System EDR** - Definicja: EDR analizuje, monitoruje oraz zapisuje informacje o działaniu systemu oraz procesów na urządzeniu końcowym (komputerze stacjonarnym lub serwerze). Dzięki wdrożonym na końcówkach agentom daje dużą widoczność i wiedzę o lokalnych zdarzeniach. Pozwala na wykrywanie zagrożeń ukrytych na przykład w pamięci komputera, co dla innych systemów jest praktycznie niemożliwe.

Funkcjonalności, które posiada system EDR:

- Przeszukiwanie incydentów i zebranych danych z końcówek
- Ocena ryzyka i różne poziomy alarmowania
- Wykrywanie podejrzanej aktywności
- Blokowanie złośliwego działania
- Integracja z innymi systemami

W skład systemu EDR wchodzą: agenty wdrożone na urządzeniach końcowych, centralny serwer zarządzający agentami oraz przetwarzający dużą ilość informacji, baza danych oraz konsola dla operatorów

Działanie systemu EDR:

Agenty monitorują na systemach lokalnych setki zdarzeń powiązanych z podejrzaną aktywnością i mogących świadczyć o zagrożeniu. Są to na przykład:

- tworzenie procesów
- ładowanie niesystemowych bibliotek
- modyfikacja rejestru
- dostęp do dysku
- połączenia sieciowe

Taki monitoring jest już dużą wartością i daje możliwość obserwowania zdarzeń typu:

- połączenia sieciowe z hostami wewnętrznymi oraz zewnętrznymi,
- zdalne oraz bezpośrednie logowania użytkowników,
- uruchamianie narzędzi administracyjnych oraz plików .exe,
- wykonywanie procesów,
- podsumowanie oraz szczegóły połączeń sieciowych (DNS, LDAP, WinRM, SMB itp.),
- tworzenie plików z określonymi rozszerzeniami,
- korzystanie z zewnętrznych nośników danych.

System EDR daje również możliwość dodatkowego zbierania informacji z urządzeń końcowych. Wywołując zapytanie, w czasie rzeczywistym możemy otrzymać następujące dane:

- listę uruchomionych procesów,
- wpisy z Windows Event Log,
- wpisy z rejestru,
- przeglądać system plików,
- pobrać zrzut pamięci z konkretnego procesu,
- wyliczyć i porównać hash pliku (hash jest ciągiem liter i cyfr o stałej długości, który można w uproszczeniu nazwać „cyfrowym odciskiem palca" pliku komputerowego),
- oraz dużo więcej za pomocą zapytań Powershell (wbudowany interpreter poleceń sytemu Windows) oraz innych wbudowanych narzędzi.

Gdy zagrożenie zostanie zdiagnozowane operatorzy mają do wyboru szeroki zestaw akcji typu „response - odpowiedź", które pozwalają na zatrzymanie lub załagodzenie złośliwego działania. Akcje takie to na przykład:

- usunięcie pliku,
- zabicie procesu,
- usunięcie lub modyfikacja klucza rejestru,
- uruchomienie skryptu/komendy,
- zaszyfrowanie/zabezpieczenie pliku lub zasobu,
- restart systemu,
- wyłączenie interfejsów sieciowych.

Zgodnie z wytycznymi konkursu, Powiaty otrzymają dofinansowanie w formie grantu do 100% wydatków kwalifikowanych. Maksymalna wysokość grantu dla jednego powiatu wynosić będzie 850 000 zł, jednym z wytycznych otrzymania grantu jest zabezpieczenie wkładu własnego w kwocie 63 978,00 zł zgodnie z Załącznikiem nr 2 - Lista podmiotów uprawnionych do uczestniczenia w naborze. W związku z powyższym łączna kwota wydatków związanych z realizacją zadania wynosi 913 978 zł brutto.

W związku z powyższym podjęcie uchwały jest zasadne.

DYREKTOR
Biura Obsługi Urzędu
Izabela Lewandowska