

Strategia rozwoju i podnoszenia poziomu bezpieczeństwa cyfrowego na lata 2023-2025 w Starostwie Powiatowym w Pile

I. Wprowadzenie

Bezpieczeństwo cyfrowe odnosi się do praktyk, technologii, środków kontroli i działań, które są implementowane w celu ochrony danych, systemów informatycznych, sieci komputerowych, urządzeń elektronicznych oraz infrastruktury cyfrowej przed zagrożeniami, atakami i nieuprawnionym dostępem. Kluczowym celem bezpieczeństwa cyfrowego jest zminimalizowanie ryzyka utraty poufności, integralności, dostępności i autentyczności informacji oraz zasobów cyfrowych.

Podstawowe elementy bezpieczeństwa cyfrowego obejmują:

- 1) ochronę przed atakami i zagrożeniami;
- 2) zarządzanie dostępem;
- 3) ochronę danych;
- 4) zabezpieczenia sieciowe;
- 5) zarządzanie ryzykiem;
- 6) zabezpieczenia fizyczne;
- 7) zabezpieczenia aplikacji;
- 8) ciągłość działania;
- 9) zgodność z przepisami i standardami;
- 10) świadomość i szkolenia.

Bezpieczeństwo cyfrowe jest dynamicznym obszarem, który stale ewoluuje w odpowiedzi na nowe technologie i zagrożenia. Skuteczne strategie bezpieczeństwa wymagają stałego monitorowania, aktualizacji oraz zaangażowania zarówno personelu IT, jak i użytkowników końcowych.

II. Diagnoza

Podnoszenie poziomu bezpieczeństwa cyfrowego jest kluczowym elementem skutecznego funkcjonowania Starostwa Powiatowego w Pile, zwłaszcza w kontekście rosnących zagrożeń związanych z cyberprzestępczością. Niniejsza strategia zakłada kompleksowe podejście do podniesienia poziomu cyberbezpieczeństwa skupiając się głównie na szkoleniach pracowników i budowaniu ich świadomości w zakresie zagrożeń wynikających ze świata cyfrowego.

Wysoki poziom bezpieczeństwa cyfrowego jest kluczowy dla Starostwa Powiatowego w Pile i obejmuje aspekty operacyjne, reputacyjne, prawne i finansowe. Bezpieczeństwo cyfrowe pomaga w ochronie aktywów organizacji, w tym danych osobowych, poufnych informacji, wizerunku firmy, a także infrastruktury informatycznej. Unikanie utraty lub skompromitowania tych aktywów jest kluczowe dla ciągłości działania. Wysoki poziom bezpieczeństwa cyfrowego pomaga w zabezpieczeniu danych, co przekłada się na zachowanie zaufania i lojalności klientów.

Przepisy prawa wymagają, aby urzędy przestrzegały określonych standardów bezpieczeństwa cyfrowego. Działania niezgodne z przepisami prawnymi mogą prowadzić do poważnych konsekwencji prawnych, w tym kar finansowych i sankcji.

Ataki cybernetyczne i incydenty bezpieczeństwa mogą generować znaczne koszty finansowe, zarówno związane z naprawą szkód, jak i stratami wynikającymi z przerw w dostępie do systemów.

Bezpieczeństwo cyfrowe jest ważne w kontekście utrzymania ciągłości działania organizacji. Ataki mogą prowadzić do przerw w działaniu, utraty dostępu do danych czy infrastruktury, co z kolei wpływa na zdolność urzędu do świadczenia usług.

Wystąpienie incydentu bezpieczeństwa może negatywnie wpłynąć na wizerunek organizacji. Wysoka widoczność w mediach społecznościowych i tradycyjnych mediach sprawia, że incydenty te są łatwo dostrzegalne przez społeczeństwo.

Utrzymanie wysokiego poziomu bezpieczeństwa cyfrowego staje się nie tylko obowiązkiem, ale także strategicznym elementem zarządzania organizacją w dynamicznie zmieniającej się rzeczywistości.

Nieświadomi pracownicy stanowią istotne zagrożenie dla bezpieczeństwa cyfrowego organizacji. Istnieje wiele potencjalnych zagrożeń wynikających z nieświadomego postępowania pracowników. Osoby nieświadome zagrożeń mogą być podatne na ataki

phishingowe, gdzie przestępcy próbują uzyskać poufne informacje, takie jak hasła, np. poprzez podszywanie się pod zaufane źródła. Kliknięcie w złośliwe linki lub otwarcie szkodliwego załącznika może prowadzić do kompromitacji systemów. Pracownicy niewystarczająco świadomi zagrożeń związanych z social engineeringiem mogą ulec manipulacji, udostępniając poufne informacje lub wykonując działania, które pozornie wydają się bezpieczne, ale są wykorzystywane przez atakujących. Niedostateczna wiedza może prowadzić do używania słabych haseł, łatwo dostępnych dla hakerów. Ponadto jeśli pracownicy używają tych samych haseł do różnych usług, atak na jedno konto może prowadzić do kompromitacji innych.

Pracownicy nieświadomi ryzyka mogą korzystać z niesankcjonowanych aplikacji lub urządzeń, wprowadzając niezabezpieczone elementy do środowiska, co zwiększa potencjalne wektory ataku. Mogą oni również ignorować lub nie zauważać sygnałów ostrzegawczych dotyczących ataków cybernetycznych, co opóźnia reakcję na incydent. Ponadto pracownicy nieświadomi zagrożeń mogą podejmować działania, które narażają na ryzyko utraty poufności danych poprzez czynności takie jak przysyłanie wrażliwych informacji drogą elektroniczną bez odpowiednich zabezpieczeń. Brak świadomości dotyczącej bezpieczeństwa sieciowego może skłaniać do korzystania z niezabezpieczonych połączeń, co stwarza ryzyko przechwycenia poufnych danych. Nieświadome postępowanie pracowników w zakresie usuwania danych może spowodować utratę ważnych informacji.

W celu zminimalizowania tych zagrożeń kluczowe jest prowadzenie regularnych szkoleń, podnoszenie świadomości pracowników i promowanie kultury bezpieczeństwa w organizacji. Wzmacnianie umiejętności rozpoznawania i reagowania na potencjalne zagrożenia cyfrowe jest ważnym elementem skutecznej strategii bezpieczeństwa cyfrowego. Szkolenia pomagają pracownikom zrozumieć różnorodne zagrożenia cyfrowe, takie jak phishing, malware, ataki typu ransomware czy socjotechniczne. Zrozumienie mechanizmów działania phishingu i jego różnych form pozwala na unikanie wejścia w podejrzane linki czy otwieranie załączników. Szkolenia powinny obejmować praktyczne wskazówki dotyczące bezpiecznych zachowań online, takich jak zasady tworzenia silnych haseł, korzystanie z autoryzowanych źródeł, aktualizowanie oprogramowania i systemów, a także bezpieczne praktyki korzystania z sieci. Integralną częścią szkoleń powinno być omówienie polityk bezpieczeństwa organizacji, w tym zasad dostępu do systemów, zarządzania danymi, korzystania z urządzeń firmowych i innych kluczowych aspektów związanych z bezpieczeństwem. Pracownicy powinni być zaznajamiani z ogólnymi zasadami bezpieczeństwa informacji, takimi jak zasada najmniejszych uprawnień czy zasada potrzeby wiedzy, aby minimalizować ryzyko naruszeń bezpieczeństwa. Szkolenia

powinny obejmować kroki jakie należy podjąć w przypadku wykrycia lub podejrzenia incydentu bezpieczeństwa. Szybka i właściwa reakcja może zminimalizować szkody wynikające z ataku. Z uwagi na dynamiczny charakter zagrożeń cyfrowych szkolenia powinny być regularnie aktualizowane, aby uwzględniać najnowsze trendy i techniki stosowane przez cyberprzestępców.

Kluczowe jest zaangażowanie pracowników w proces budowania bezpieczeństwa. Organizacje mogą inicjować konkursy, nagradzać za bezpieczne praktyki, czy nawet tworzyć programy nagród dla tych, którzy wnoszą istotny wkład w ochronę cybernetyczną. Pracownicy powinni być zachęceni do natychmiastowego zgłaszania wszelkich podejrzanych sytuacji lub incydentów bezpieczeństwa, aby umożliwić szybką reakcję.

Starostwo Powiatowe w Pile może znacząco poprawić swoje bezpieczeństwo cyfrowe poprzez systematyczne i kompleksowe szkolenia pracowników, tworząc tym samym świadomych i aktywnych uczestników w procesie ochrony przed cyberzagrożeniami.

III. Cele i działania

1) Podniesienie ogólnej świadomości:

Cele:

- a) zwiększenie ogólnej świadomości pracowników na temat zagrożeń cyfrowych;
- b) wdrożenie stałego procesu edukacji w zakresie cyberbezpieczeństwa.

Działania:

- a) przeprowadzenie regularnych kampanii informacyjnych;
- b) organizacja prelekcji i szkoleń wewnętrznych na temat cyberzagrożeń.

2) Zaawansowane szkolenia pracowników:

Cele:

- a) kształtowanie umiejętności rozpoznawania zaawansowanych ataków;
- b) wzrost zdolności reakcji na incydenty bezpieczeństwa.

Działania:

- a) organizacja zaawansowanych szkoleń z zakresu cyberbezpieczeństwa dla kadry IT;
- b) symulacje ataków i scenariuszy incydentów.

3) Szkolenia wstępne dla nowych pracowników - integracja zabezpieczeń cyfrowych w procesie onboardingu:

Cele:

- a) wprowadzenie nowych pracowników w zasady bezpieczeństwa cyfrowego;
- b) zapewnienie wiedzy na temat polityk bezpieczeństwa organizacji.

Działania:

- a) przygotowanie systemu e-learningowego i udostępnienie go pracownikom;
- b) opracowanie materiałów szkoleniowych na potrzeby onboardingu;
- c) przeprowadzenie indywidualnych szkoleń dla nowozatrudnionych.

4) Kampanie edukacyjne i świadomościowe - cykliczne kampanie bezpieczeństwa:

Cele:

- a) regularne przypominanie pracownikom o zasadach bezpieczeństwa;
- b) budowanie kultury bezpieczeństwa cyfrowego.

Działania:

- a) kampanie mailingowe związane z aktualnymi zagrożeniami;
- b) wykorzystanie różnorodnych mediów i form przekazu.

5) Edukacja wewnętrzna:

Cele:

- a) działania skupione na wewnętrznej specyfice organizacji;
- b) integracja wiedzy o specyfice instytucji w kampaniach edukacyjnych.

Działania:

- a) opracowanie scenariuszy i przypadków specyficznych dla Starostwa;
- b) szkolenia dostosowane do specyfiki pracy poszczególnych działów.

IV. Monitorowanie i ewaluacja

1) Wskaźniki:

- a) procent pracowników uczestniczących w szkoleniach;
- b) czas reakcji na zgłaszane incydenty bezpieczeństwa;
- c) liczba zgłoszonych fałszywych alarmów;
- d) ilość szkoleń dodanych do systemu elearningowego;
- e) ilość szkoleń specjalistycznych dla pracowników IT.

2) Monitorowanie:

- a) regularne raportowanie z uczestnictwa w szkoleniach;

- b) analiza czasu reakcji i skuteczności procedur incydentowych;
- c) badanie satysfakcji i efektywności szkoleń;
- d) ocena poziomu satysfakcji pracowników z przeprowadzonych szkoleń;
- e) analiza efektywności wdrożonych działań edukacyjnych;
- f) ankiety satysfakcji po zakończonych szkoleniach.

V. Kontrola i działania zapobiegawcze

1) Przeprowadzanie cyklicznych audytów bezpieczeństwa i zgodności z KRI

Cele:

- a) regularne oceny i aktualizacje polityk bezpieczeństwa;
- b) identyfikacja nowych zagrożeń i dostosowywanie procedur.

Działania:

- a) przeprowadzanie corocznych audytów bezpieczeństwa;
- b) przeprowadzanie wewnętrznych sprawdzeń przestrzegania zapisów dokumentacji bezpieczeństwa;
- c) uaktualnianie polityk w oparciu o wyniki audytów.

2) Dostosowywanie procedur do nowych zagrożeń:

Cele:

- a) dynamiczne dostosowywanie procedur w związku z nowymi zagrożeniami;
- b) zapobieganie incydentom poprzez świadome działania;

Działania:

- a) reaktywne modyfikacje procedur na podstawie analizy incydentów;
- b) proaktywne dostosowywanie w oparciu o analizę trendów.

VI. Realizacja, zadania i odpowiedzialności

W ramach realizacji Strategii rozwoju i podnoszenia poziomu bezpieczeństwa cyfrowego na lata 2023-2025 w Starostwie Powiatowym w Pile udział i odpowiedzialność poszczególnych wydziałów są kluczowe dla skutecznego jej wdrożenia.

Biuro Kadr i Plac odpowiedzialne jest za:

- 1) pozyskanie zewnętrznych usług szkoleniowych dla pracowników;
- 2) pozyskanie zewnętrznych zaawansowanych usług szkoleniowych dla pracowników IT;
- 3) administracyjną obsługę i dokumentowanie przebiegu szkoleń.

Wydział Funduszy Pomocowych i Rozwoju odpowiedzialny jest za:

- 1) pozyskiwanie zewnętrznych środków finansowych mogących wspomóc realizację strategii;
- 2) identyfikację dostępnych funduszy;
- 3) monitorowanie źródeł finansowania, takich jak dotacje, fundusze europejskie, czy inne formy wsparcia finansowego;
- 4) przygotowywanie wniosków o finansowanie, zgodnie z wymaganiami różnych programów i źródeł finansowania;
- 5) nawiązywanie kontaktów i negocjacje z partnerami zewnętrznymi oraz instytucjami finansującymi.

Wydział Informatyki odpowiedzialny jest za:

- 1) przygotowanie środowiska dla systemu e-learningowego;
- 2) współpracę przy przygotowaniu i wdrożeniu systemu e-learningowego;
- 3) utrzymanie i udostępnianie pracownikom systemu e-learningowego.

Wydział Administracyjny odpowiedzialny jest za:

- 1) administrowanie procesami związanymi z wdrożeniem strategii;
- 2) koordynację zespołu odpowiedzialnego za wdrożenie strategii;
- 3) zarządzanie czasem i zasobami;
- 4) efektywne planowanie środków własnych na wdrożenie poszczególnych etapów strategii;
- 5) zapewnienie przejrzystej i skutecznej komunikacji wewnętrznej w kontekście zmian wynikających ze strategii.

VII. Podsumowanie

Strategia obejmuje szeroki zakres działań, od podstawowych szkoleń dla nowych pracowników po zaawansowane kursy dla specjalistów IT. Kampanie edukacyjne i świadomościowe mają na celu kształtowanie trwałej kultury bezpieczeństwa cyfrowego. Monitorowanie i ewaluacja zapewnią, że podejmowane działania są efektywne, a system jest dynamicznie dostosowywany do zmieniającego się środowiska cybernetycznego. Cykliczne audyty i adaptacyjne procedury mają służyć zapobieganiu incydentom oraz szybkiemu reagowaniu na nowe zagrożenia.