Dla firm

Cyberbezpieczeństwo

instytucji publicznych

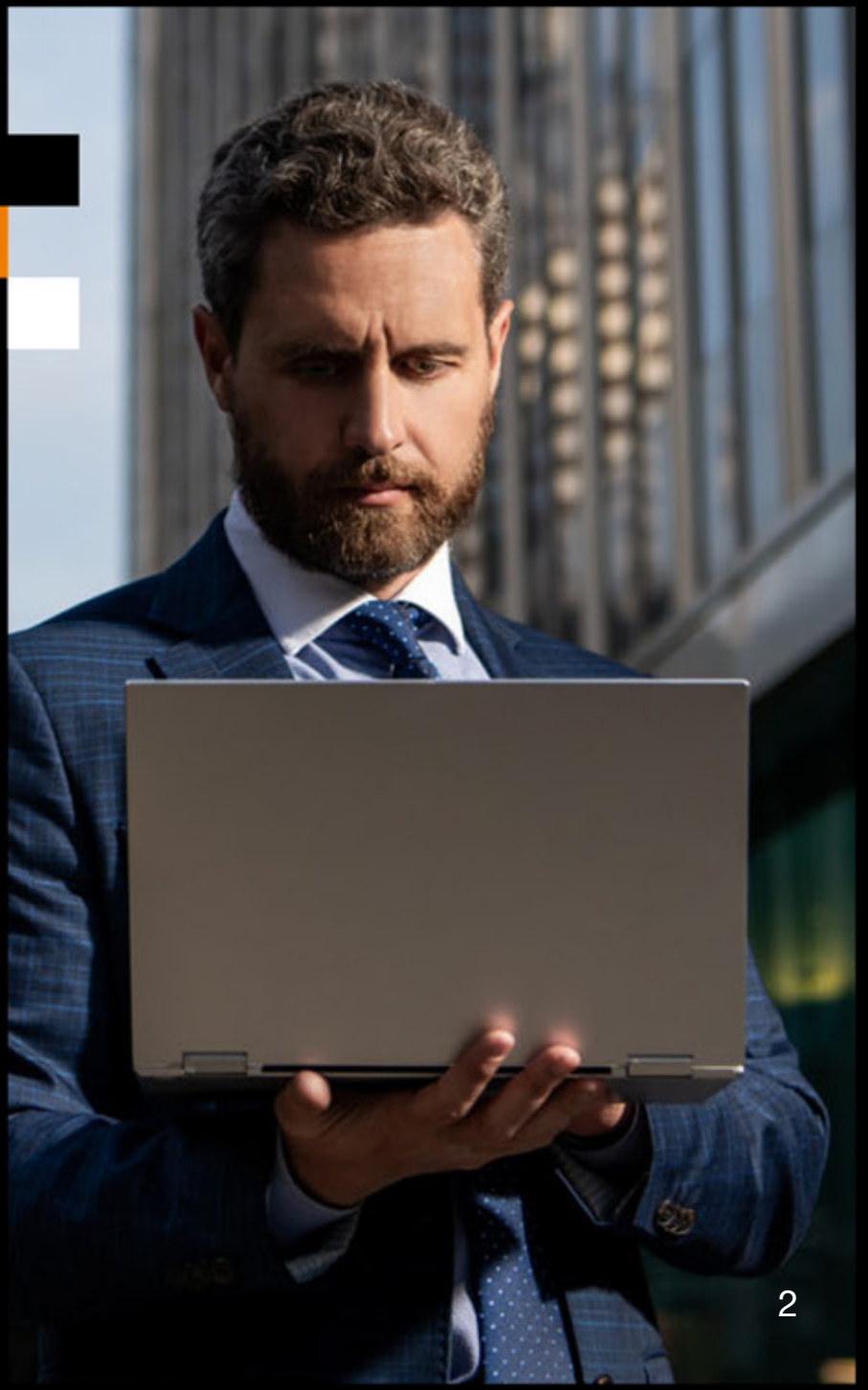
Jak chronić dane i prywatność obywateli?

orange™
tu jest

Zapewnienie odpowiedniego poziomu cyberbezpieczeństwa instytucji publicznych jest sprawą priorytetową

Z tego względu trzeba poznać mechanizmy, narzędzia i plany działania, które pomogą im w skutecznej obronie przed współczesnymi zagrożeniami.

Niniejszy e-book udowadnia, dlaczego cyberbezpieczeństwo powinno być kluczowym elementem uwagi każdej instytucji publicznej.



Instytucje publiczne w obliczu cyberzagrożeń

Cyberprzestrzeń stała się nową areną globalnych zmagań, na której każdego dnia, m.in. instytucje publiczne stawiają czoło niewidzialnym wrogom. Zjawisko nielegalnych praktyk w cyberprzestrzeni rozwija się równie dynamicznie, co sama technologia.

Najnowsze **badania wskazują na alarmujący wzrost liczby ataków hakerskich,** naruszeń danych i innych działań z zakresu cyberprzestępczości. Nie jest to jedynie problem dużych organizacji rządowych. Potencjalnymi celami są również mniejsze podmioty, takie jak lokalne urzędy, a nawet pojedynczy interesanci. Konsekwencje naruszeń bezpieczeństwa mogą być rozmaite **– od strat finansowych po utratę reputacji.**

Instytucje publiczne doskonale znają ten problem, a inicjatywy takie jak „Cyfrowa gmina” czy „Cyberbezpieczny samorząd” pokazują, że traktują go bardzo poważnie. Tylko ciągła edukacja, wdrażanie transformacji cyfrowej i wzmacnianie cyberochrony mogą skutecznie zapobiegać kolejnym, coraz to nowocześniejszym atakom.

Aktualne statystyki i dane dotyczące ataków

Dotykając problematyki zagrożeń, z jakimi podmioty publiczne zmagają się każdego dnia na globalną skalę, trudno przejść obojętnie obok alarmujących statystyk.

Z analizy firmy Check Point Research wynika, że od początku 2024 roku organizacje w Polsce atakowane są średnio 1 800 razy w tygodniu - dotyczy to głównie administracji publicznej i wojska.

Co warte dodania, średni koszt pojedynczego incydentu dla małego podmiotu oceniany jest na – bagatela – 200 tysięcy dolarów (w przypadku dużych organizacji ta kwota sięga nawet miliona dolarów!). Ranking zagrożeń rokrocznie otwierają incydenty cybernetyczne takie jak:

- phishing
- ataki DDoS
- ransomware
- naruszenia danych spowodowane przez zaawansowane trwałe zagrożenia (Advanced Persistent Threats, APT)

Cyberataki na instytucje publiczne w liczbach

68,9%

instytucji publicznych przyznaje, że w I kwartale 2023 roku odnotowało przynajmniej jeden incydent cyberbezpieczeństwa

średnio co

9 minut

atakowana jest instytucja publiczna

zaledwie

26,4%

badanych podmiotów ma przygotowane procedury na wypadek ataku hakerskiego

670

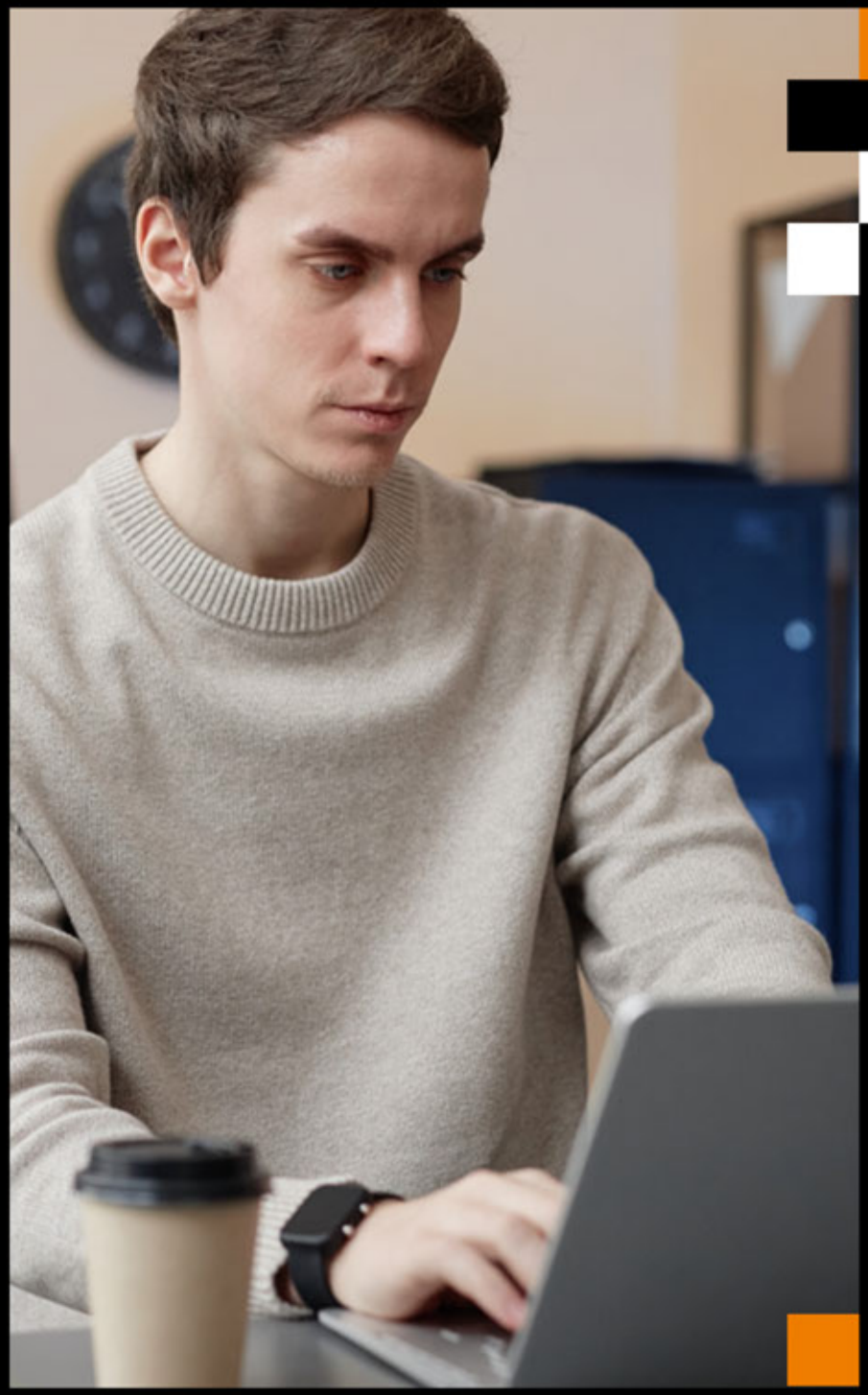
tys. zł

to wysokość przeciętnego okupu za odszyfrowanie danych

500%

o tyle w 2023 roku wzrosła liczba ataków na polski sektor użyteczności publicznej, względem roku 2022

Źródła: Check Point Research, VECTO, Sophos



Rodzaje zagrożeń

Niebezpieczeństwa w przestrzeni wirtualnej ewoluują w zaskakującym tempie. Cyberprzestępcy i oszuści wykorzystują coraz bardziej zaawansowane techniki oraz socjotechniki, aby obejść zabezpieczenia.

Ataki phishingowe, a zwłaszcza ich zaawansowana odmiana – spear-phishing, stanowią poważne wyzwanie dla świata biznesu. Aby wyłudzić cenne informacje, przestępcy rozsyłają wiadomości e-mail lub SMS, **podszywając się pod współpracowników czy instytucje publiczne.** W rzeczywistości są to starannie przygotowane pułapki. Kliknięcie w link lub otwarcie załącznika prowadzi do zainstalowania na urządzeniu zainfekowanego oprogramowania.

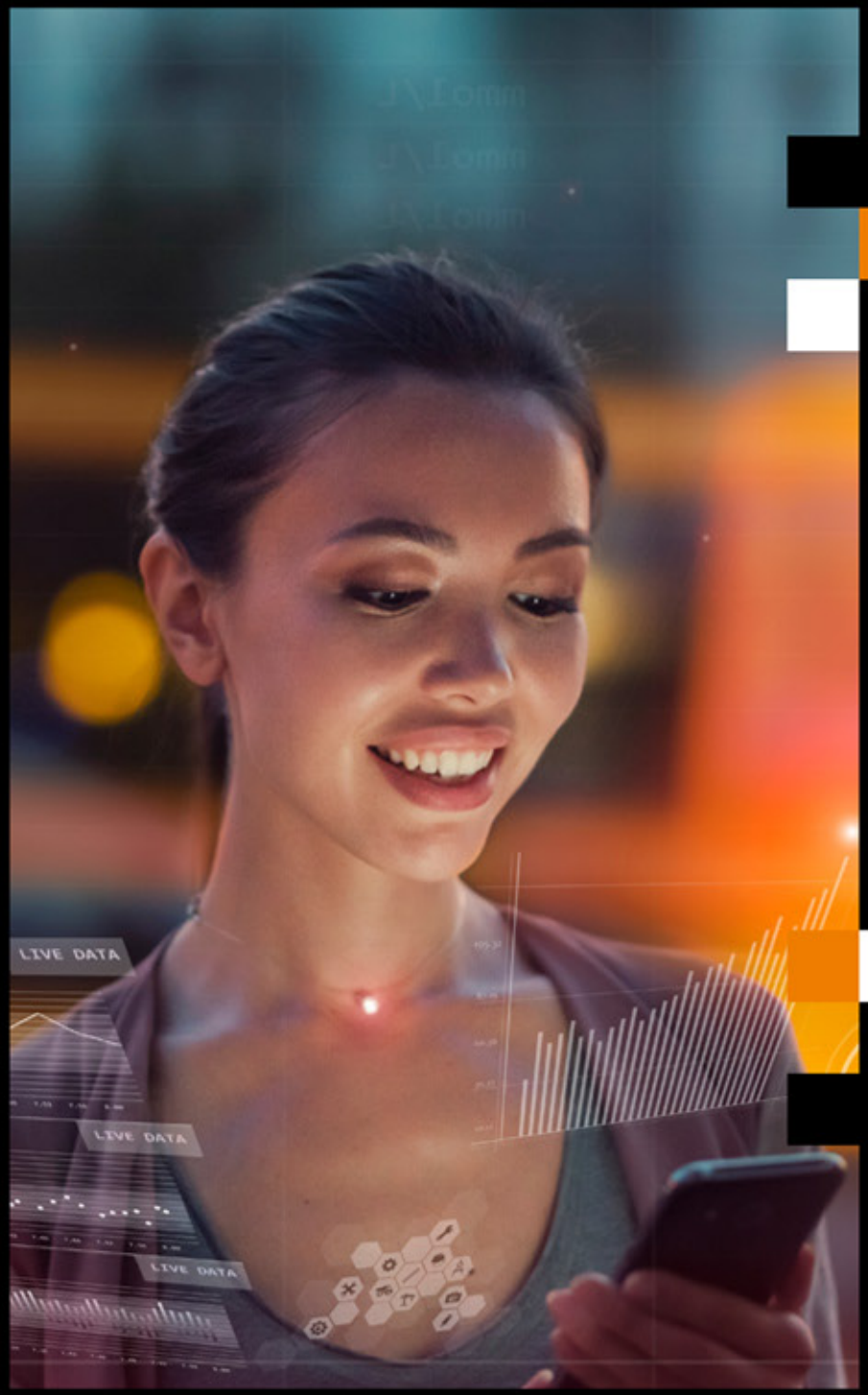
Ransomware - taki atak polega na zaszyfrowaniu danych ofiary i wymuszeniu okupu za ich odblokowanie. Zgodnie z raportem Fortinet **aż dwie trzecie różnego rodzaju organizacji było celem ataków ransomware w 2022 roku.** Szczególnie niepokojące jest to, że w przypadku połowy tych incydentów cyberprzestępcy osiągnęli sukces, skutecznie forsując systemy zabezpieczeń.

Ataki typu Man-in-the-Middle (MitM) polegają na podsłuchiwaniu lub modyfikowaniu komunikacji między dwoma stronami, co **może prowadzić do kradzieży poufnych informacji i poważnego naruszenia prywatności.** Cyberprzestępcy przeprowadzają je na różne sposoby – poprzez fałszowanie adresów IP, DNS, HTTPS, ARP czy tworzenie wrogich punktów dostępowych.

Jak dbać o cyberbezpieczeństwo?

Coraz bardziej wysublimowane metody ataków stawiają przed instytucjami publicznymi nowe wyzwania. Nie chodzi już tylko o ochronę mienia, ale przede wszystkim wirtualnych zasobów.

Dane to nowa waluta cyfrowego świata, a ich wyciek może być równie szkodliwy i kosztowny jak kradzież fizycznych aktywów.



Najsłabszym ogniwem jest… człowiek

Często okazuje się, że najsłabszym punktem systemu zabezpieczeń jest właśnie człowiek. Pracownicy mogą nieświadomie narazić instytucję na wiele zagrożeń. Dzieje się tak, jeśli nie przestrzegają zasad i procedur dotyczących bezpiecznego korzystania z systemów i danych. Wśród najczęściej popełnianych błędów, które zagrażają bezpieczeństwu wewnętrznemu, wymienia się:

- Otwieranie załączników z nieznanych źródeł, które mogą zawierać szkodliwe oprogramowanie.
- Klikanie w podejrzane linki, które mogą prowadzić do stron phishingowych lub złośliwych skryptów.
- Przynoszenie na pendrivie lub dyskach złośliwego oprogramowania, które może zainfekować komputer, a nawet całą sieć służbową.
- Przekazywanie danych logowania, które mogą być wykorzystane przez osoby nieuprawnione do uzyskania dostępu do służbowych systemów i danych.
- Przekazywanie hasła do poczty w odpowiedzi na wiadomość e-mail osoby podszywającej się pod pracownika działu IT, przez co możliwe jest przejęcie kontroli nad kontem i wysyłanie fałszywych wiadomości.
- Zapisywanie haseł na kartkach, które mogą być zgubione, skradzione lub przechwycone przez osoby niepowołane.
- Stosowanie haseł typu „qwerty”, „admin1” itp., które są łatwe do odgadnięcia lub złamania przez hakerów.

Świadomość jako pierwsza linia obrony

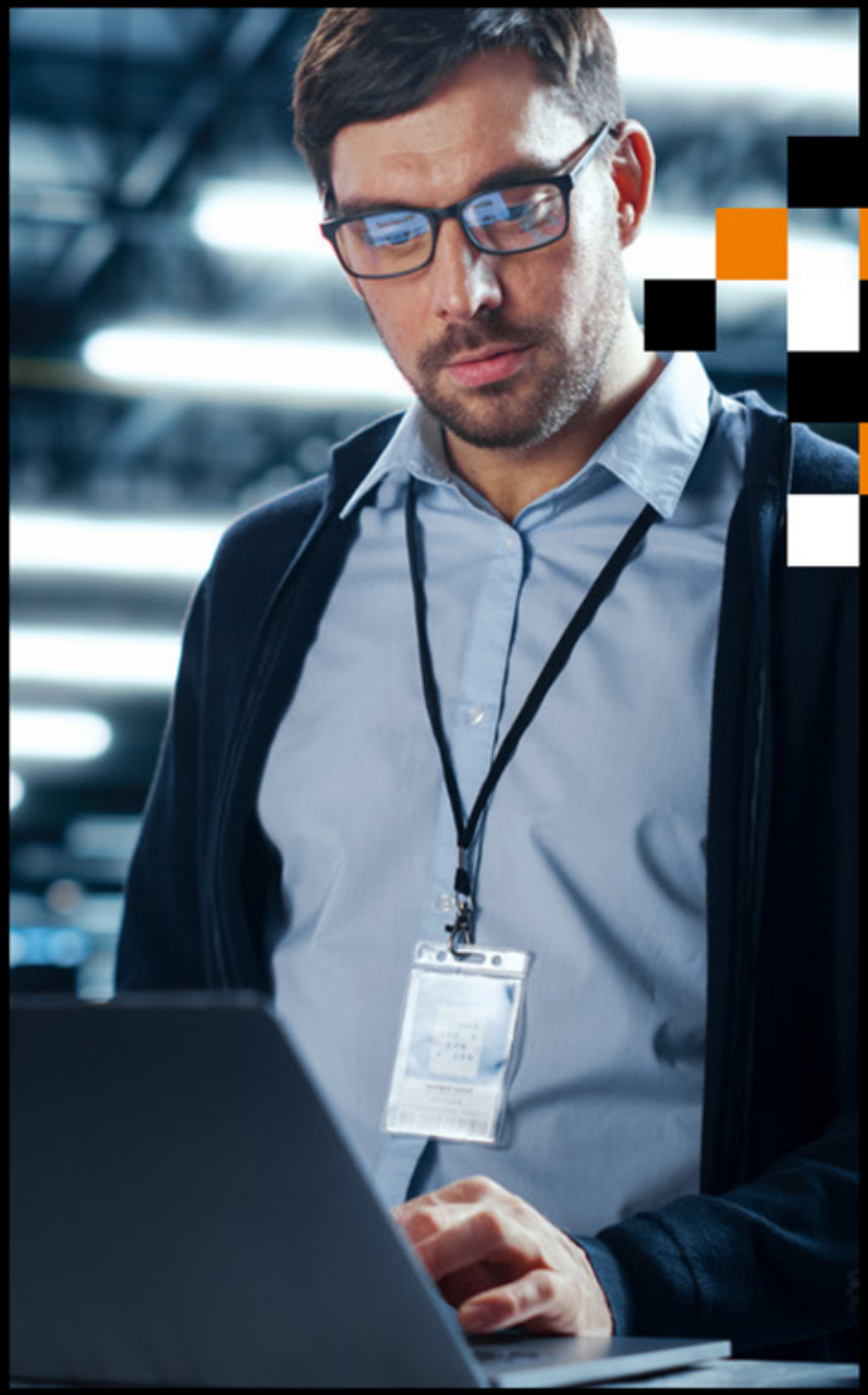
Przeciwdziałanie cyberatakom powinno zaczynać się od edukacji i podnoszenia świadomości zarówno wśród dyrektorów, jak i pracowników. Wspieranie inicjatyw edukacyjnych i dostęp do aktualnej wiedzy w dziedzinie cyberbezpieczeństwa to podstawowe kroki, które mogą mieć znaczny wpływ na poprawę bezpieczeństwa całej instytucji.

Cyberświadomość to także krytyczne myślenie i podejmowanie przemyślanych decyzji. Każdy pracownik powinien zdawać sobie sprawę z możliwego ryzyka związanego z używaniem technologii. Ważne jest też, aby **był gotowy podjąć odpowiednie działania w celu minimalizacji tego zagrożenia.**

Czy zastanawiasz się, jak zwiększyć ochronę przetwarzanych danych i bezpieczeństwo systemów?

Mamy dla Ciebie rozwiązanie!

Na stronie Cyberbezpieczny samorząd znajdziesz kompleksowe usługi, które pozwolą Ci spać spokojnie.



Profilaktyka cyberbezpieczeństwa

Jak mówi przysłowie ,,lepiej zapobiegać niż leczyć", a w kontekście bezpieczeństwa informacji jest to złota reguła. Profilaktyka w cyberbezpieczeństwie obejmuje nie tylko zabezpieczenia techniczne, ale również szereg działań prewencyjnych.

Każdy pracownik powinien mieć dostęp wyłącznie do tych zasobów, które są niezbędne do wykonywania jego obowiązków. W celu respektowania tych zasad warto wdrożyć system zarządzania tożsamością i dostępem IAM (ang. Identity and Access Management).

Ochrona przed cyberzagrożeniami obejmuje zabezpieczenie fizyczne urządzeń. Kontrola dostępu do pomieszczeń ze sprzętem IT, zamki, alarmy czy kamery to podstawowe środki ochrony sprzętu przed nieuprawnionym ich wykorzystaniem.

Kluczowym elementem profilaktyki jest również stworzenie przemyślanej i zrozumiałej dla wszystkich pracowników PBI (Polityka Bezpieczeństwa Informacji), będącej częścią SZBI (System Zarządzania Bezpieczeństwem Informacji). Dokument ten powinien zawierać procedury postępowania w przypadku wykrycia naruszenia czy instrukcje zgłaszania incydentów.

Regularne przeprowadzanie testów phishingowych i symulacji ataków phishingowych pozwala na weryfikację skuteczności wprowadzonych zabezpieczeń oraz przygotowanie pracowników na różne scenariusze incydentów bezpieczeństwa.

Możemy lepiej chronić dane instytucji, pracowników i interesantów poprzez:

korzystanie z wirtualnych sieci prywatnych (VPN) zaprojektowanych w celu ochrony danych podczas ich przesyłania

wdrożenie uwierzytelniania wieloskładnikowego w celu zapobiegania nieautoryzowanemu dostępowi

regularne aktualizowanie systemów operacyjnych, urządzeń i oprogramowania

wybieranie silnych haseł zawierających kombinację cyfr, symboli oraz dużych i małych liter

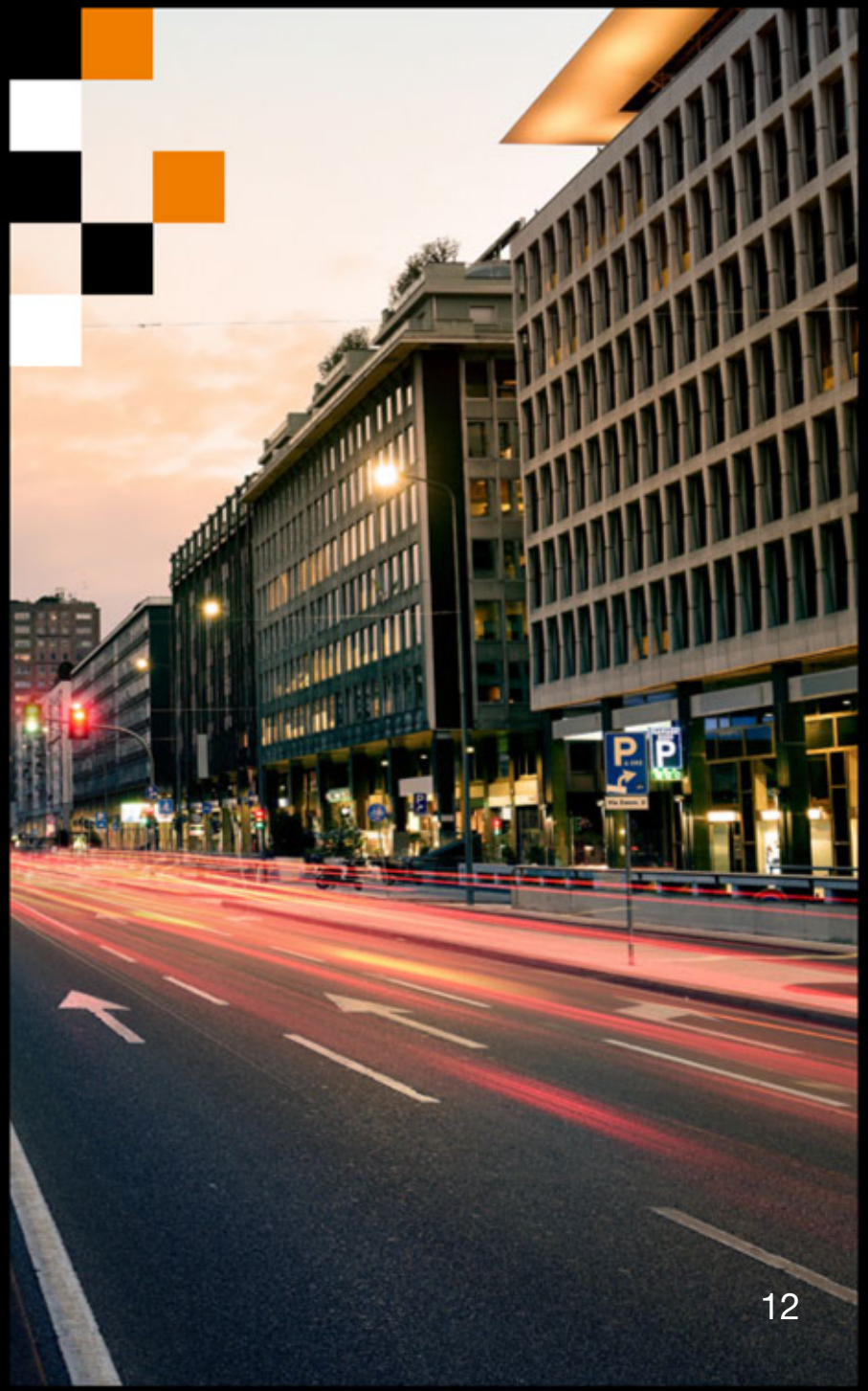
regularnie tworzenie kopii zapasowych i przechowywanie ich poza siedzibą placówki – najlepiej w chmurze

Smart City – troska o cyberbezpieczeństwo

Do tej pory omawialiśmy najważniejsze praktyki z zakresu ochrony danych w instytucjach publicznych. Pora, aby spojrzeć szerzej na miejskie ekosystemy, które wykorzystują zaawansowane technologie, np. czujniki, znaczniki i urządzenia internetu rzeczy (IoT). **Również te elementy są narażone na ataki, które mogą mieć poważne konsekwencje** dla mieszkańców i całej infrastruktury miejskiej.

Czym są inteligentne miasta?

Smart Cities, czyli inteligentne miasta, **to koncepcja, która zmienia tradycyjne pojmowanie urbanistyki.** Jej kluczowe elementy prezentujemy poniżej.



Zaawansowane technologie informacyjno-komunikacyjne – inteligentne miasta korzystają z najnowszych osiągnięć w obszarze IT/ICT, które stają się rdzeniem ich funkcjonowania. Obejmuje to zarówno rozbudowaną infrastrukturę sieciową, czujniki, kamery (urządzenia IoT), jak i zaawansowanie systemy analizujące dane w czasie rzeczywistym.

Zintegrowane systemy zarządzania – są to platformy oparte na architekturze chmurowej, które zbierają i przetwarzają dane z różnych źródeł. Pozwalają one na szybką reakcję na wydarzenia w mieście i optymalizację procesów takich jak: ruch drogowy, zarządzanie odpadami czy zapewnienie bezpieczeństwa publicznego.

Wysoki poziom automatyzacji – w inteligentnych miastach wiele funkcji jest zautomatyzowanych. Przykładem mogą być inteligentne sieci energetyczne (smart grids). Automatycznie wskazują one zapotrzebowaniem na energię czy też systemy transportowe, które regulują ruch w zależności od aktualnych potrzeb i warunków.

Zrównoważony rozwój – koncepcja Smart City zakłada redukowanie śladu węglowego poprzez efektywne wykorzystanie zasobów i promowanie ekologicznych rozwiązań, takich jak elektromobilność czy inteligentne systemy zarządzania wodą i energią.

Smart City - wyzwania

Rozwój internetu rzeczy (IoT) oraz chmury obliczeniowej przyniósł kolejne wyzwania dla samorządów i instytucji publicznych, otwierając nowe furtki dla cyberprzestępców. **Każde połączone z internetem urządzenie może stać się potencjalnym celem** dla hakerów.

Systemy zarządzania ruchem, miejskie sieci Wi-Fi, zdalnie odczytywane liczniki **– to tylko niektóre rozwiązania mogące działać w oparciu o nasze rozwiązania chmurowe. Spełniają one najwyższe standardy jakości, a także oferują solidne zabezpieczenia przed cyberatakami.**

Niemniej należy pamiętać, że kluczową strategią w zabezpieczaniu inteligentnych miast jest tzw. projektowanie z myślą o bezpieczeństwie (ang. security by design). Oznacza to, że zabezpieczenia cybernetyczne powinny być wprowadzane już na etapie planowania i wdrażania systemów, a nie dodawane po fakcie.

W maju 2021 roku w Stanach Zjednoczonych doszło do poważnego cyberataku, który uderzył w infrastrukturę krytyczną. Atak ransomware na Colonial Pipeline, jeden z największych operatorów rurociągów paliwowych w USA, sparaliżował systemy zarządzające siecią przesyłową ropy i paliw. Cyberprzestępcy z grupy DarkSide, wykorzystując złośliwe oprogramowanie, zablokowali dostęp do danych i wymusili okup. W wyniku tego ataku, dostawy paliwa zostały wstrzymane, co doprowadziło do poważnych zakłóceń w zaopatrzeniu stacji benzynowych oraz wywołało panikę i wzrost cen paliw w wielu stanach.

Atak na Colonial Pipeline pokazał, jak w dzisiejszym świecie złośliwe oprogramowanie może wpływać na codzienne życie obywateli oraz podkreślił pilną potrzebę wzmocnienia zabezpieczeń w sektorze infrastruktury krytycznej.

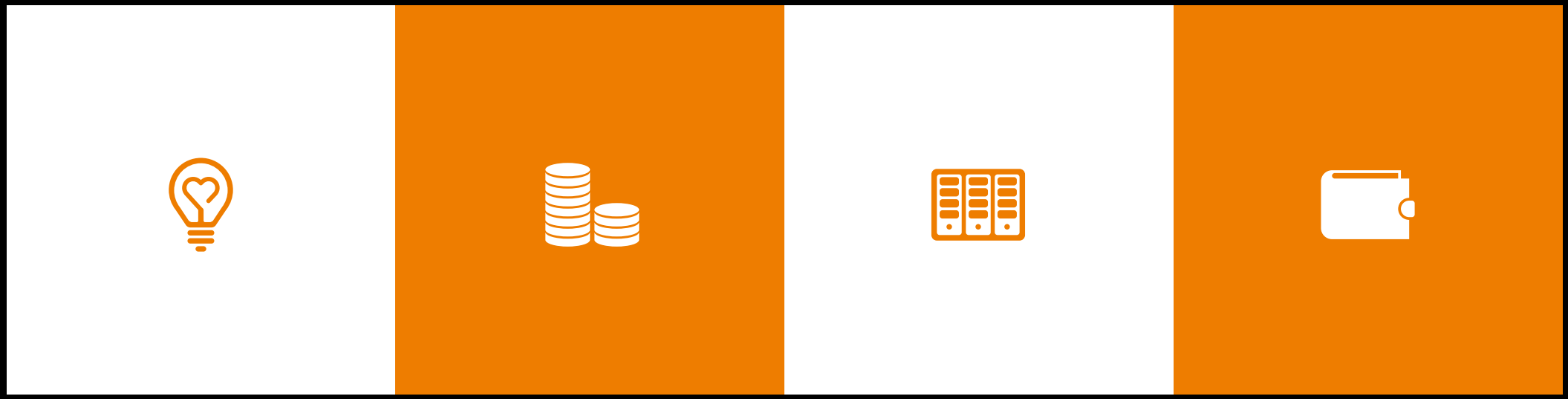
Outsourcing – bezpieczeństwo instytucji w rękach specjalistów

Kompleksowa ochrona krytycznej infrastruktury IT może być kosztowna i złożona. Nie wszystkie instytucje publiczne dysponują odpowiednimi zasobami finansowymi lub technicznymi, by skutecznie chronić się przed zagrożeniami.

Odpowiedzią na te wyzwania jest outsourcing. To rozwiązanie dla sektora publicznego, który bardzo często zmaga się z brakiem kadr oraz wysokimi kosztami rekrutacji i utrzymania wewnętrznych działów IT.

Outsourcing usług bezpieczeństwa pozwala na przejęcie odpowiedzialności za cyberbezpieczeństwo przez wyspecjalizowane firmy, takie jak Orange. Przynosi to wiele korzyści.

Organizacje poprzez outsourcing usług bezpieczeństwa mogą:



korzystać z najnowszych technologii i wiedzy doświadczonych ekspertów

przewidywać budżet na cyberbezpieczeństwo oraz eliminować niespodziewane wydatki dzięki opcji stałego abonamentu

zwiększyć efektywność i skalowalność swoich działań w zakresie ochrony danych i systemów informatycznych

uniknąć strat finansowych w wyniku ataków hakerskich lub naruszeń bezpieczeństwa

Jak to działa?

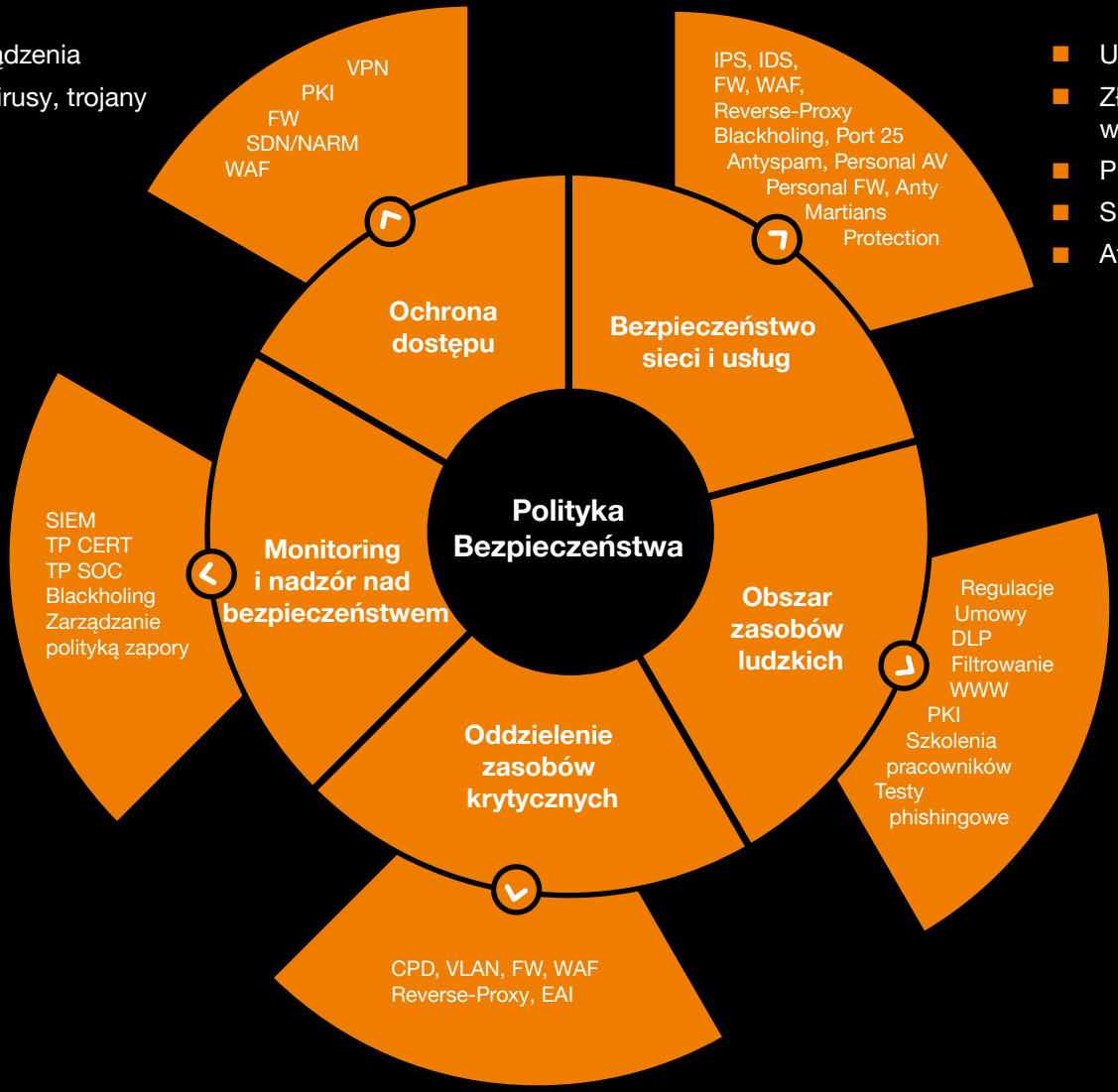
Proces outsourcingu bezpieczeństwa IT można porównać do wynajęcia doświadczonego ogrodnika, którego zadaniem jest regularne dbanie o ogród. Na czym polega podobieństwo? Korzystając z usług zewnętrznych dostawców, **otrzymujesz dostęp do specjalistycznej wiedzy ekspertów**, którzy monitorują i chronią zasoby przed potencjalnymi zagrożeniami. Wszystko to w ramach miesięcznej subskrypcji ze stałą opłatą.

Zakres outsourcingu usług bezpieczeństwa może obejmować różnorodne obszary, zależnie od potrzeb i priorytetów instytucji. Najczęściej są to takie działania jak:

- monitoring sieci
- zarządzanie zabezpieczeniami i dostępem
- reagowanie na incydenty
- audyt i raportowanie
- analiza ryzyka
- szkolenia pracowników i testy phishingowe

Holistyczne podejście do bezpieczeństwa w Orange Polska

- Nieautoryzowane użycie urządzenia
- Złośliwe oprogramowanie, wirusy, trojany
- Ataki hakerskie



- Utrata dostępności
- Złośliwe oprogramowanie, wirusy, trojany
- Phishing
- Spam
- Ataki hakerskie

- Utrata dostępności
- Ujawnienie informacji
- Nadużycie autoryzacji
- Kradzież danych
- Phishing
- Spam
- Złośliwe oprogramowanie, wirusy, trojany
- Ataki hakerskie

- Kradzież danych
- Złośliwe oprogramowanie, wirusy, trojany
- Podsłuch
- Szpiegostwo

- Niedostępność usług krytycznych
- Ujawnienie informacji

Cyberbezpieczny samorząd z Orange

Orange oferuje usługi przygotowane z myślą o jednostkach samorządu terytorialnego. Pomagają one w budowaniu odpornej infrastruktury IT i chronią dane przed cyberatakami.

Ochrona przed atakami DDoS

Jednym z kluczowych zagrożeń dla jednostek samorządu terytorialnego (JST) są ataki typu DDoS. Mogą one sparaliżować strony internetowe i uniemożliwić mieszkańcom dostęp do kluczowych usług. Orange oferuje usługę Orange Internet Protection (OIP), która zapewnia:

- **Ciągłość działania kluczowych procesów** – OIP chroni serwisy internetowe JST przed atakami DDoS, zapewniając ich dostępność dla mieszkańców.
- **Szybką reakcję na zagrożenie** – usługa wykorzystuje zaawansowane technologie do monitorowania ruchu sieciowego i błyskawicznego reagowania na ataki.
- **Eksperckie wsparcie** – zespół Orange Security Operations Center (SOC) jest dostępny 24/7, aby zapewnić JST niezbędne wsparcie w przypadku ataku.

CyberPakiet – kompleksowe wsparcie w cyberbezpieczeństwie

CyberPakiet to usługa, która rozszerza kompetencje działów IT JST w zakresie cyberbezpieczeństwa. Obejmuje ona:

Automatyczne i manualne narzędzia – CyberPakiet automatyzuje wiele zadań związanych z cyberbezpieczeństwem.

Ochronę urządzeń – usługa chroni urządzenia działające w sieci stacjonarnej i mobilnej przed złośliwym oprogramowaniem.

Skanowanie podatności – CyberPakiet regularnie, raz w miesiącu, skanuje systemy JST w poszukiwaniu luk bezpieczeństwa i pomaga w ich usuwaniu.

Edukację i budowanie świadomości – CyberPakiet obejmuje również programy edukacyjne dla pracowników JST, które pomagają im w rozpoznawaniu i unikaniu cyberzagrożeń.

Podsumowanie

W dobie postępującej transformacji cyfrowej nie można bagatelizować potencjalnych zagrożeń związanych z cyberprzestrzenią. Zapewnienie bezpieczeństwa cyfrowego obejmuje nie tylko stosowanie odpowiednich technologii, ale również angażowanie ludzi i skuteczne procesy.

Aby sprostać wyzwaniom cyfrowej transformacji, instytucje muszą opracować i wdrożyć strategię cyberbezpieczeństwa. Powinna ona opierać się na czterech filarach: zapobieganiu, wykrywaniu, reagowaniu i odzyskiwaniu.

Pamiętaj – **w cyberbezpieczeństwie nie ma miejsca na zbytnią pewność siebie.** Tylko poprzez świadome podejście do identyfikacji, zrozumienia i reagowania na nowe zagrożenia możesz skutecznie zabezpieczyć organizację przed atakami cybernetycznymi.

www.orange.pl/poradnik-dla-firm

orange™
tu jest