KRAJOWY PLAN ODBUDOWY

Rzeczpospolita Polska

Sfinansowane przez Unię Europejską NextGenerationEU

NASK

Ministerstwo Cyfryzacji

COI Centralny Ośrodek Informatyki

Jak dobrze wykorzystać EZD RP i zapewnić bezpieczeństwo systemu

– moderowany panel z zaproszonymi ekspertami wsparcia i usług SaaS

Daniel Ciesnowski – Kierownik Zespołu Service Desk EZD

Przedsięwzięcie pn.: „Wsparcie dla powszechnego stosowania elektronicznego zarządzania dokumentacją poprzez rozwój i udostępnienie nieodpłatnego systemu klasy EZD, udostępnienie chmury SaaS2 EZD RP oraz wdrożenia systemu EZD w administracji publicznej RP” realizowane jest przez Ministerstwo Cyfryzacji w partnerstwie z NASK-PIB w ramach Krajowego Planu Odbudowy i Zwiększania Odporności, finansowanego ze środków Instrumentu na rzecz Odbudowy i Zwiększenia Odporności oraz Unii Europejskiej – NextGenerationEU.

1
bezpieczna codzienna praca

2
najczęstsze ryzyka i błędy

3
odpowiedzialność użytkownika

**Teza: bezpieczeństwo EZD RP nie kończy się na technologii.
Zaczyna się tam, gdzie użytkownik podejmuje codzienną decyzję:
komu daję dostęp, co wysyłam, gdzie pracuję i jak reaguję na błąd.**

NASK

EZD RP to nie tylko narzędzie do pisma

To środowisko pracy na dokumentach, sprawach, zadaniach, korespondencji i integracjach.

dokumenty	**sprawy**	**zadania**	**komunikacja**	**podpisy**

Bezpieczeństwo danych i kontrola dostępu muszą działać w całym obiegu - od wpływu dokumentu po archiwizację i wysyłkę.

- integracje m.in. z ePUAP, e-Doręczeniami i KSeF
- system wspiera obieg dokumentów w małych i dużych jednostkach
- skuteczność zależy od poprawnej konfiguracji i pracy użytkowników

NASK

Bezpieczeństwo to łańcuch odpowiedzialności

Najsłabsze ogniwo często nie jest techniczne – bywa nim proces albo rutyna użytkownika.

Operator SaaS	Instytucja	Administrator	Użytkownik
ciągłość, infrastruktura, dostęp usługi	polityki, sieć, administratorzy, urządzenia	role, uprawnienia, konta, reakcja	hasło, dokument, odbiorca, stanowisko

Panel ma sens wtedy, gdy łączymy perspektywę wsparcia, usług SaaS i realnej pracy użytkownika.

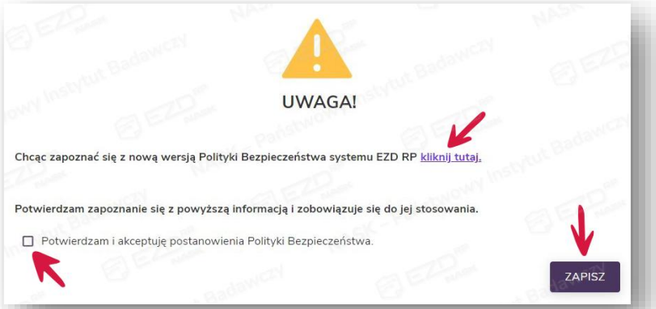
NASK

Co użytkownik realnie chroni?

W codziennej pracy chronimy nie tylko konto, ale także kontekst sprawy i ścieżkę decyzji.

Tożsamość	Dokument	Odbiorców
login, hasło, MFA, sesja, blokada ekranu	treść, załączniki, metadane, historia czynności	prawidłowy adresat, właściwy kanał, brak pomyłek

Stanowisko	Zaufanie
urządzenie, sieć, drukarka, skaner, nośniki	spójność procesu i wiarygodność urzędu



NASK

Dobra praktyka 1: konto i stanowisko

Najprostsze zachowania często blokują najpoważniejsze scenariusze nadużyć.

- nie udostępniaj konta, hasła ani aktywnej sesji – nawet „na chwilę”,
- blokuj ekran przy odejściu od stanowiska,
- nie zapisuj haseł w notatnikach, arkuszach i wspólnych plikach,
- nie pracuj na prywatnym lub niesprawdzonym sprzęcie, jeśli polityka tego nie dopuszcza,
- zgłaszaj utratę urządzenia, podejrzane logowanie lub nietypowe zachowanie systemu.

Zasada: konto użytkownika = podpis pod działaniem w systemie.

NASK

Dobra praktyka 2: dokument i adresat

Największe ryzyko bywa banalne: właściwy dokument trafia do niewłaściwej osoby.

przed wysłaniem

- odbiorca
- załącznik
- podstawa wysyłki

w trakcie pracy

- klasyfikacja
- uprawnienia
- wersja dokumentu

po czynności

- potwierdzenia
- historia sprawy
- ewentualna korekta

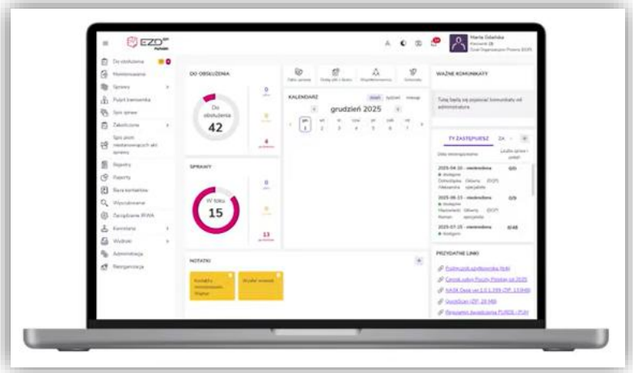
Minimum kontroli: „Czy ta osoba powinna zobaczyć dokładnie ten dokument, w tej wersji, w tym kanale?”

Dobra praktyka 3: praca zdalna i mobilna

Zdalny dostęp musi być tak samo kontrolowany jak praca w urzędzie.

Urządzenie poza siecią urzędu = większa odpowiedzialność za kanał, ekran i otoczenie.

- korzystaj wyłącznie z zatwierdzonego sposobu dostępu zdalnego,
- unikaj pracy w miejscach, w których treść dokumentów widzą osoby postronne,
- nie przenoś dokumentów do prywatnych chmur, komunikatorów i poczty prywatnej,
- aktualizuj system, przeglądarkę i zabezpieczenia urządzenia,
- po zakończeniu pracy wyloguj się i zamknij sesję.



NASK

Uprawnienia: mniej znaczy bezpieczniej

Dostęp powinien wynikać z obowiązków służbowych i stanowiska - nie z wygody.

- regularny przegląd uprawnień,
- szablony zgodne ze strukturą organizacyjną,
- natychmiastowe blokowanie dostępu po ustaniu potrzeby,
- nie eskaluj uprawnień „na zapas”.

Uprawnienia są elementem bezpieczeństwa, ale również jakości procesu.

NASK

Najczęstsze ryzyka i błędy

W praktyce bezpieczeństwo najczęściej przegrywa z pośpiechem, rutyną i skrótami.

Pomyłka odbiorcy

wysyłka dokumentu lub załącznika do niewłaściwej osoby

Nadmiar uprawnień

użytkownik widzi więcej, niż potrzebuje do pracy

Udostępnianie konta

brak rozliczalności czynności w systemie

Prywatne kanały

pliki poza kontrolą organizacji

Phishing

fałszywe linki, podszywanie się, wyłudzenia dostępu

Brak reakcji

problem znany, ale niezgłoszony na czas

Gdy coś pójdzie nie tak: reakcja użytkownika

Szybka reakcja ogranicza skalę skutków. Ukrywanie błędu zwykle ją zwiększa.

1. Zatrzymaj	2. Zabezpiecz	3. Zgłoś	4. Współpracuj
nie kontynuuj czynności, nie kasuj śladów	zrób notatkę: co, kiedy, komu, jaki dokument	zgodnie z procedurą jednostki i kanałem wsparcia	odpowiadaj na pytania, nie powielaj błędu

- numer sprawy lub zgłoszenia,
- data i przybliżona godzina,
- nazwa czynności i skutki,
- zrzut ekranu tylko wtedy, gdy procedura na to pozwala.

Wymagania dostępu do SaaS EZD RP – w skrócie

Użytkownik powinien rozumieć, dlaczego dostęp do systemu jest kontrolowany na poziomie instytucji.

Whitelist	IPSec VPN Site-to-Site	Praca mobilna
dostęp tylko z zatwierdzonych publicznych adresów IP	szyfrowany tunel między siecią instytucji a infrastrukturą operatora	zatwierdzony VPN Point-to-Site i kierowanie ruchu przez sieć instytucji

NASK

Wiedza użytkownika to zabezpieczenie

Podręcznik, szkolenia i wsparcie ograniczają liczbę błędów operacyjnych.

Podręcznik użytkownika	Filmy i materiały	Kursy e-learningowe
szybki dostęp do instrukcji, wzorów, szablonów i informacji technicznych	pokazują najważniejsze czynności w systemie w zwięzły sposób	systematyzują wiedzę kancelaryjną i procesową

Najbezpieczniejszy użytkownik to nie ten, który wszystko pamięta. To ten, który wie, gdzie sprawdzić procedurę przed wykonaniem ryzykownej czynności.

NASK

Najkrócej: 5 zachowań, które robią różnicę

1. chroń konto i sesję
2. weryfikuj adresata i załącznik
3. pracuj tylko zatwierdzonym kanałem dostępu
4. zgłaszaj błędy od razu
5. ucz się z podręcznika i procedur

Dziękuję.
Zapraszamy do udziału w panelu z ekspertami,

Most do panelu: pytania do ekspertów

Propozycje pytań, które naturalnie rozwijają temat bezpieczeństwa i dobrego wykorzystania EZD RP.

- Jakie błędy użytkowników najczęściej generują ryzyko albo zgłoszenia do wsparcia?
- Jak jednostka powinna organizować przeglądy uprawnień i obsługę zmian kadrowych?
- Co jest dziś największym wyzwaniem przy pracy zdalnej i dostępie do SaaS EZD RP?
- Jakie informacje w zgłoszeniu najbardziej przyspieszają reakcję wsparcia?
- Co po wdrożeniu powinno być mierzone: zgłoszenia, jakość danych, czas obsługi, szkolenia?

KRAJOWY PLAN ODBUDOWY

Rzeczpospolita Polska

Sfinansowane przez Unię Europejską NextGenerationEU

NASK

Ministerstwo Cyfryzacji

COI Centralny Ośrodek Informatyki

Dziękuję za uwagę

Daniel Ciesnowski – Kierownik Zespołu Service Desk EZD

Przedsięwzięcie pn.: „Wsparcie dla powszechnego stosowania elektronicznego zarządzania dokumentacją poprzez rozwój i udostępnienie nieodpłatnego systemu klasy EZD, udostępnienie chmury SaaS2 EZD RP oraz wdrożenia systemu EZD w administracji publicznej RP” realizowane jest przez Ministerstwo Cyfryzacji w partnerstwie z NASK-PIB w ramach Krajowego Planu Odbudowy i Zwiększania Odporności, finansowanego ze środków Instrumentu na rzecz Odbudowy i Zwiększenia Odporności oraz Unii Europejskiej – NextGenerationEU.