DLA ZARZĄDU

Żuraw Transport sp. z o.o.: co o firmie widać z internetu

NR RAPORTU	DATA	ZAKRES	ANALITYK
SW-SCAN-2611-007	21.11.2026	3 domeny · 9 adresów IP	M. Nowak

F

OCENA

A B C D F

Dwa problemy pozwalają dziś wejść do sieci firmy z internetu

Firewall z dostępem VPN ma znaną lukę, którą przestępcy aktywnie wykorzystują, a jeden serwer przyjmuje logowanie pulpitu zdalnego z całego świata. To najczęstsze drogi ataków ransomware na średnie firmy. Oba problemy da się zamknąć w kilka dni.

2	4	5	3
krytyczne	wysokie	średnie	niskie

Stan na 20.11.2026. Raport nie jest audytem ani oceną zgodności z ustawą o KSC. Ograniczenia: strona 5.

5 najważniejszych ryzyk

1 Firewall z luką wykorzystywaną przez przestępców — KRYTYCZNE

Bramka VPN działa na wersji oprogramowania z podatnością z listy CISA KEV (CVE-2024-21762). Pozwala przejąć urządzenie bez logowania.

2 Pulpit zdalny dostępny z internetu — KRYTYCZNE

Serwer przyjmuje logowanie RDP z dowolnego miejsca na świecie. Wystarczy jedno zgadnięte albo wykradzione hasło.

3 Hasła 3 pracowników w logach złośliwego oprogramowania — WYSOKIE

Na trzech komputerach (prywatnych albo służbowych) działał program kradnący hasła. Wśród danych jest konto z dostępem do poczty działu księgowości.

4 Każdy może wysłać e-mail „od prezesa” — WYSOKIE

Domena nie blokuje podszywania się (DMARC w trybie obserwacji). To otwiera drogę do oszustw na fałszywą fakturę.

5 Kod strony testowej z kluczem do bramki SMS — WYSOKIE

Na serwerze testowym jest dostępna cała historia kodu, a w niej aktywny klucz API do wysyłki SMS.

Ścieżka pilna: ryzyka 1 i 2 przekazaliśmy telefonicznie p. Annie Wiśniewskiej 20.11.2026 o 15:40, zanim powstał ten raport.

DLA DZIAŁU IT

Wszystkie ustalenia

ID	USTALENIE	ZASÓB	WAGA	ART. 8 UKSC
K-01	FortiOS 7.2.4 na bramce SSL VPN, podatność CVE-2024-21762 (lista CISA KEV)	vpn.zuraw-transport.example 203.0.113.10	KRYTYCZNE	podatności, aktualizacje
K-02	RDP (3389/tcp) otwarty na internet, brak ograniczenia adresów	203.0.113.24	KRYTYCZNE	kontrola dostępu
W-01	3 konta firmowe w logach infostealerów z ostatnich 6 miesięcy	zuraw-transport.example	WYSOKIE	kontrola dostępu, MFA
W-02	DMARC `p=none`, SPF kończy się `~all`	zuraw-transport.example	WYSOKIE	bezpieczna komunikacja
W-03	Publicznie dostępny katalog `.git`, w historii aktywny klucz API bramki SMS	staging.zuraw-transport.example	WYSOKIE	bezpieczeństwo rozwoju systemów
W-04	Subdomena wskazuje na usuniętą usługę w chmurze (możliwe przejęcie subdomeny)	promo.zuraw-transport.example	WYSOKIE	zarządzanie aktywami
S-01	Serwer poczty przyjmuje TLS 1.0 i 1.1	poczta.zuraw-transport.example	ŚREDNIE	kryptografia
S-02	Panel administracyjny WordPress dostępny z internetu bez ograniczeń	www.zuraw-transport.example/wp-admin	ŚREDNIE	kontrola dostępu
S-03	Zarejestrowana podobna domena z rekordem MX (możliwy phishing)	zuraw-transpprt.example	ŚREDNIE	cyberhigiena, edukacja
S-04	41 adresów firmowych w publicznych wyciekach (2019–2024)	zuraw-transport.example	ŚREDNIE	kontrola dostępu
S-05	Certyfikat TLS wygasa za 12 dni	sklep.zuraw-transport.example	ŚREDNIE	ciągłość działania
N-01	Brak nagłówków bezpieczeństwa (HSTS, CSP)	www, sklep	NISKIE	bezpieczeństwo rozwoju systemów
N-02	Serwery www ujawniają wersje oprogramowania	www, staging	NISKIE	cyberhigiena
N-03	Brak rekordu CAA w DNS	zuraw-transport.example	NISKIE	kryptografia

Waga według realnego ryzyka: podatności z listy CISA KEV i usługi otwarte na internet ważą więcej niż sama ocena CVSS. Kolumna „Art. 8 UKSC” wskazuje obszar środków bezpieczeństwa z art. 8 ustawy o krajowym systemie cyberbezpieczeństwa, którego dotyczy ustalenie.

DLA DZIAŁU IT

Ustalenia krytyczne i wysokie: szczegóły

K-01 Bramka VPN z podatnością CVE-2024-21762 — KRYTYCZNE

CO WIDZIMY	Baner i odpowiedź interfejsu SSL VPN wskazują na FortiOS 7.2.4. Ta wersja ma podatność pozwalającą wykonać kod bez logowania; CISA potwierdza jej aktywne wykorzystanie.
DLACZEGO WAŻNE	Przejęcie firewalla daje napastnikowi wejście do sieci wewnętrznej i ominięcie MFA.
CO ZROBIĆ	Aktualizacja FortiOS do wersji poprawionej przez producenta; do czasu aktualizacji wyłączenie SSL VPN. Po aktualizacji sprawdzenie urządzenia pod kątem śladów przejęcia (narzędzie producenta).
JAK SPRAWDZILIŚMY	Rozpoznanie wersji bez prób wykorzystania podatności.

K-02 Pulpit zdalny otwarty na internet — KRYTYCZNE

CO WIDZIMY	Port 3389/tcp odpowiada na 203.0.113.24, certyfikat RDP z nazwą `SRV-FK01` (prawdopodobnie serwer finansowo-księgowy).
CO ZROBIĆ	Zamknięcie portu na firewallu; dostęp zdalny tylko przez VPN z MFA, po aktualizacji z K-01. Przegląd logów logowania na serwerze z ostatnich 90 dni.

W-01 Konta w logach infostealerów — WYSOKIE

CO WIDZIMY	3 konta, w tym konto działu księgowości. Logi zawierają adresy stron, na których wpisano dane, m.in. logowanie do poczty Microsoft 365 i bankowości. Listę kont przekazujemy osobno, tylko osobie uprawnionej.
CO ZROBIĆ	Reset haseł i unieważnienie sesji tych kont, sprawdzenie komputerów, z których wykradziono dane, wymuszenie MFA dla wszystkich kont.

W-02 Domena nie chroni przed podszywaniem — WYSOKIE

CO WIDZIMY	`v=DMARC1; p=none` oraz SPF `~all`. Wiadomości podszywające się pod domenę firmy trafiają do odbiorców.
CO ZROBIĆ	Przegląd raportów DMARC przez 2 tygodnie, potem `p=quarantine`, docelowo `p=reject`; SPF zakończony `-all`.

W-03 Historia kodu na serwerze testowym — WYSOKIE

CO WIDZIMY	`/.git/` zwraca konfigurację repozytorium; w historii zmian jest klucz API bramki SMS (aktywny według odpowiedzi API, bez jego użycia).
CO ZROBIĆ	Unieważnienie klucza i wydanie nowego, usunięcie katalogu `.git` z serwera, ograniczenie dostępu do środowiska testowego.

W-04 Subdomena do przejęcia — WYSOKIE

CO WIDZIMY	`promo` ma rekord CNAME na nieistniejący zasób w chmurze. Ktokolwiek założy zasób o tej nazwie, opublikuje treść pod adresem firmy.
CO ZROBIĆ	Usunięcie rekordu CNAME albo odtworzenie zasobu.

PLAN DZIAŁAŃ

Co zrobić w ciągu 30 dni

Tydzień 1

- K-01: aktualizacja FortiOS, kontrola śladów przejęcia
- K-02: zamknięcie RDP, dostęp przez VPN z MFA
- W-01: reset haseł, sprawdzenie komputerów
- W-03: nowy klucz API, usunięcie `.git`

Tydzień 2

- W-04: usunięcie rekordu `promo`
- W-02: zbieranie raportów DMARC, poprawa SPF
- S-05: odnowienie certyfikatu
- MFA dla wszystkich kont Microsoft 365

Tydzień 3–4

- W-02: DMARC `p=quarantine`
- S-01: wyłączenie TLS 1.0 i 1.1
- S-02: ograniczenie `/wp-admin`
- S-03: zgłoszenie podobnej domeny, ostrzeżenie dla pracowników

Po wdrożeniu poprawek wykonamy bezpłatnie ponowny skan (do 60 dni od tego raportu) i przygotujemy raport „przed i po”.

Odniesienie do ustawy o KSC

Jeśli Żuraw Transport jest podmiotem kluczowym albo ważnym, art. 8 ustawy o krajowym systemie cyberbezpieczeństwa wymaga m.in. zarządzania podatnościami i regularnych aktualizacji, kontroli dostępu, bezpiecznej komunikacji z uwierzytelnianiem wieloskładnikowym oraz kryptografii. Ustalenia K-01, K-02, W-01 i W-02 dotyczą bezpośrednio tych obszarów.

Czy firma podlega ustawie, sprawdzimy w trakcie omówienia raportu. Transport należy do sektorów z załącznika nr 1 do ustawy. Obowiązki trzeba wdrożyć do 3 kwietnia 2027 r., jeśli firma spełniała przesłanki 3 kwietnia 2026 r.

ZAKRES I METODA

Jak powstał ten raport

Zgoda	Podpisana elektronicznie 19.11.2026 przez p. Annę Wiśniewską (prokurent, KRS). Własność domen potwierdzona rekordem TXT.
Domeny	`zuraw-transport.example`, `zuraw.example`, `zuraw-sklep.example`; 18 subdomen
Adresy IP	9 adresów w bloku 203.0.113.0/27; 2 adresy hostingu współdzielonego wyłączone z zakresu
Skan aktywny	20.11.2026, 9:00–15:00, z adresu 198.51.100.7 (`scanner.secwolf.pl`). 1000 najczęstszych portów, limit 300 pakietów/s, tylko testy nieinwazyjne.
Poza zakresem	Sieć wewnętrzna, Active Directory, konfiguracja Microsoft 365 od środka, aplikacje za logowaniem, próby logowania i wykorzystania podatności. Skan pokazuje tylko to, co widać z zewnątrz.
Dane osobowe	Listy wyciekłych kont usuniemy 21.12.2026. Zgodę i log skanu przechowujemy jako dowód, że skan był uprawniony.
Narzędzia	subfinder, dnsx, crt.sh, checkdmarc, naabu, httpx, nuclei, testssl.sh, dnstwist, trufflehog, Shodan, Have I Been Pwned
Kontrola raportu	Analityk: M. Nowak · Sprawdził: K. Lis

Ograniczenia raportu

Raport opisuje stan na dzień skanu (20.11.2026) i obejmuje tylko domeny i adresy wymienione w zakresie. Skan był zewnętrzny i nieinwazyjny, dlatego brak ustaleń nie oznacza braku podatności. Ocena od A do F nie jest audytem, certyfikatem ani oceną zgodności z ustawą o krajowym systemie cyberbezpieczeństwa i nie stanowi porady prawnej. Część ustaleń opiera się na rozpoznaniu wersji oprogramowania, a producent mógł usunąć podatność bez zmiany numeru wersji, dlatego przed wprowadzeniem zmian zalecamy ich potwierdzenie. Dane o wyciekach pochodzą z publicznych i komercyjnych źródeł zewnętrznych, które mogą być niepełne; znalezionych danych logowania nie używaliśmy. Zalecenia wdraża klient lub jego dostawca IT, po przetestowaniu. Raport jest poufny i przeznaczony wyłącznie dla adresata. Skan wykonano na podstawie zgody z 19.11.2026 i na warunkach w niej określonych, w tym dotyczących odpowiedzialności.

Ocena od A do F: A, brak ustaleń wysokich i krytycznych; B, tylko średnie; C, co najmniej jedno wysokie; D, kilka wysokich albo aktywne konta w logach infostealerów; F, co najmniej jedno krytyczne.