§

CYBERBEZPIECZEŃSTWO

SPIS TREŚCI:

---

1) DLACZEGO PUBLIKUJEMY TĘ ZAKŁADKĘ

1. JCHost.pl świadczy usługi hostingu, poczty e-mail, serwerów dedykowanych, rejestracji domen i certyfikatów SSL. Jako podmiot świadczący usługi rejestracji nazw domen jesteśmy podmiotem kluczowym w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa i w związku z tym udostępniamy Ci wiedzę o cyberzagrożeniach związanych z naszymi usługami oraz o skutecznych sposobach zabezpieczania się przed nimi. Na tej stronie znajdziesz także informację, jak zgłosić nam cyberzagrożenie, incydent lub podatność.
2. Bezpieczeństwo Twojej strony, poczty i domeny zależy od obu stron. My dbamy o bezpieczeństwo infrastruktury, filtrowanie spamu i ochronę przed atakami na nasze systemy, a w usługach hostingu i poczty także o kopie zapasowe w zakresie opisanym w regulaminie (na serwerze dedykowanym kopie zapasowe wykonujesz samodzielnie). Ty odpowiadasz za hasła, aktualność oprogramowania zainstalowanego na hostingu lub serwerze dedykowanym oraz za bezpieczeństwo urządzeń, z których korzystasz.

2) NAJCZĘSTSZE ZAGROŻENIA I JAK SIĘ PRZED NIMI CHRONIĆ

1. **Phishing i podszywanie się pod JCHost.pl.** Oszuści rozsyłają wiadomości e-mail i SMS-y wyglądające jak wiadomości od dostawcy hostingu: o rzekomym wygaśnięciu domeny, zaległej fakturze, przepełnionej skrzynce albo konieczności „weryfikacji konta”. Odnośnik prowadzi do fałszywej strony logowania lub płatności, a jej celem jest wyłudzenie hasła albo danych karty. Jak się chronić: nie loguj się i nie płać przez odnośniki z wiadomości – wpisz adres panel.jchost.pl samodzielnie w przeglądarce; sprawdź adres nadawcy i adres strony w pasku przeglądarki; w razie wątpliwości zadzwoń do nas na numer podany na stronie Kontakt. Nigdy nie prosimy o podanie hasła w wiadomości ani przez telefon.
2. **Przejęcie konta w Panelu Klienta lub skrzynki pocztowej.** Najczęstszą przyczyną są słabe lub powtarzane hasła, które wyciekły z innego serwisu, oraz złośliwe oprogramowanie na komputerze. Przejęte konto pozwala napastnikowi zmienić dane domeny, przekierować stronę albo rozsyłać spam z Twojej skrzynki. Jak się chronić: używaj długich, unikalnych haseł (najlepiej z menedżera haseł), włącz weryfikację dwuetapową wszędzie tam, gdzie jest dostępna (w usłudze Poczty JCHost.pl jest dostępna), nie udostępniaj danych logowania innym osobom i zmieniaj hasło po każdym podejrzeniu wycieku.
3. **Włamanie na stronę internetową.** Strony oparte na systemach takich jak WordPress, Magento czy PrestaShop są przejmowane głównie przez nieaktualne wtyczki, motywy i wersje systemu, słabe hasła do panelu administracyjnego i konta FTP oraz pozostawione na serwerze nieużywane skrypty. Skutkiem bywa umieszczenie na stronie złośliwego kodu, przekierowań, stron phishingowych albo skryptów rozsyłających spam, co prowadzi do zablokowania strony przez przeglądarki i dostawców poczty. Jak się chronić: aktualizuj system, wtyczki i motywy na bieżąco, usuwaj nieużywane dodatki, stosuj osobne, silne hasła do panelu administracyjnego i konta FTP, łącz się przez SFTP lub FTPS zamiast zwykłego FTP, ogranicz liczbę kont administracyjnych i regularnie sprawdzaj stronę pod kątem nieznanych plików.
4. **Złośliwe oprogramowanie i ransomware na Twoim komputerze.** Zainfekowany komputer administratora strony jest najprostszą drogą do kradzieży haseł FTP, poczty i Panelu Klienta oraz do zaszyfrowania plików z

żądaniem okupu. Jak się chronić: aktualizuj system operacyjny i przeglądarkę, korzystaj z programu antywirusowego, nie otwieraj załączników i makr z nieznanych źródeł, nie instaluj oprogramowania spoza oficjalnych źródeł i przechowuj własną kopię zapasową strony oraz poczty poza serwerem (kopie zapasowe wykonywane w ramach hostingu są dostępne przez ograniczony czas i nie zastępują własnego archiwum).

5. **Ataki na pocztę e-mail: spam, spoofing i przejęcie skrzynki.** Przejęta skrzynka służy do rozsyłania spamu i oszustw w Twoim imieniu, a podszycie się pod Twoją domenę (spoofing) jest możliwe, gdy domena nie ma poprawnie skonfigurowanych rekordów SPF, DKIM i DMARC. Jak się chronić: skonfiguruj rekordy SPF, DKIM i DMARC dla swojej domeny (usługa Poczty JCHost.pl je obsługuje), włącz weryfikację dwuetapową w poczcie, nie używaj tego samego hasła do poczty i do innych serwisów, zachowaj ostrożność wobec załączników i odnośników, także w wiadomościach od znanych nadawców.
6. **Przejęcie domeny (domain hijacking).** Napastnik próbuje przenieść domenę do innego rejestratora albo zmienić jej abonenta, wykorzystując przejętą skrzynkę e-mail abonenta, wyłudzony kod authinfo albo nieaktualne dane kontaktowe, które uniemożliwiają nam kontakt z Tobą. Jak się chronić: dbaj o aktualność danych abonenta w Panelu Klienta (imię i nazwisko lub nazwa, adres, telefon, e-mail), zabezpiecz skrzynkę e-mail przypisaną do domeny, nigdy nie przekazuj kodu authinfo osobom trzecim ani w odpowiedzi na wiadomość e-mail, a każdą prośbę o zmianę danych lub transfer domeny, której nie zleciłeś, zgłoś nam niezwłocznie. Weryfikacja danych abonentów, którą prowadzimy zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, służy między innymi ochronie przed takimi próbami – dlatego odpowiadaj na nasze wiadomości weryfikacyjne.
7. **Ataki DDoS.** Atak polega na zalaniu serwera ruchem, który uniemożliwia lub utrudnia działanie strony. W razie ataku podejmujemy dostępne nam działania ograniczające jego skutki, w miarę możliwości technicznych po stronie infrastruktury. Jak się chronić: utrzymuj lekką, dobrze zoptymalizowaną stronę z mechanizmami pamięci podręcznej, rozważ usługę sieci dostarczania treści (CDN) z ochroną przed DDoS dla stron o dużym ruchu, a w razie zauważenia nietypowego spowolnienia lub niedostępności strony zgłoś to nam.
8. **Nieaktualne oprogramowanie na serwerze dedykowanym.** W przypadku serwera dedykowanego administrujesz systemem samodzielnie. Nieaktualny system operacyjny, otwarte niepotrzebne porty, dostęp SSH z hasłem zamiast klucza i brak zapory sieciowej to najczęstsze przyczyny włamań. Jak się chronić: instaluj aktualizacje bezpieczeństwa, ogranicz dostęp administracyjny do wybranych adresów IP i uwierzytelniania kluczem, włącz zaporę i monitoring logowań, wykonuj własne kopie zapasowe i przechowuj je poza serwerem.
9. **Socjotechnika i oszustwo „na fakturę" lub „na pracownika".** Napastnik podszywa się pod kontrahenta, przełożonego albo dostawcę usług i nakłania do przelewu na zmieniony numer rachunku lub do przekazania danych dostępowych. Jak się chronić: każdą zmianę numeru rachunku, prośbę o pilny przelew lub o dane logowania potwierdzaj innym kanałem (na przykład telefonicznie pod znanym Ci numerem), a nasze płatności realizuj wyłącznie na podstawie proform dostępnych w Panelu Klienta.

3) DZIESIĘĆ ZASAD BEZPIECZNEGO KORZYSTANIA Z USŁUG JCHOST.PL

1. Do każdej usługi używaj innego, długiego hasła; przechowuj hasła w menedżerze haseł.
2. Włączaj weryfikację dwuetapową wszędzie tam, gdzie jest dostępna.
3. Loguj się do Panelu Klienta wyłącznie pod adresem panel.jchost.pl wpisanym samodzielnie, nie przez odnośniki z wiadomości.
4. Aktualizuj system zarządzania treścią, wtyczki, motywy i oprogramowanie na serwerze niezwłocznie po wydaniu aktualizacji.
5. Łącz się z serwerem przez SFTP lub FTPS, a z serwerem dedykowanym – przez SSH z kluczem.
6. Przechowuj własną kopię zapasową strony, bazy danych i poczty poza serwerem i sprawdzaj, czy da się ją odtworzyć.
7. Skonfiguruj dla domeny rekordy SPF, DKIM i DMARC oraz certyfikat SSL dla strony.
8. Utrzymuj aktualne dane abonenta domeny i odpowiadaj na nasze wiadomości weryfikacyjne.
9. Nie przekazuj nikomu kodu authinfo, haseł ani kodów jednorazowych – nie prosimy o nie w wiadomościach ani telefonicznie.
10. Zgłaszaj nam każde podejrzenie incydentu, zagrożenia lub podatności – im szybciej, tym mniejsze skutki.

§

4) JAK ROZPOZNAĆ PRAWDZIWĄ WIADOMOŚĆ OD JCHOST.PL

1. Wiadomości od JCHost.pl wysyłamy wyłącznie z adresów w domenie jchost.pl (w szczególności: biuro@jchost.pl, bok@jchost.pl, admin@jchost.pl, rozliczenia@jchost.pl). Wiadomość z innej domeny, nawet zawierająca nasze logo, nie pochodzi od nas. Nie dotyczy to wiadomości operatorów płatności, z których korzystamy (wskazanych w regulaminie i w Panelu Klienta), ani wiadomości weryfikacyjnych wysyłanych przez Rejestr domeny .pl (NASK).
2. Płatności za usługi realizowane są na podstawie proform udostępnianych w Panelu Klienta pod adresem panel.jchost.pl. Wiadomość z żądaniem zapłaty przez odnośnik prowadzący poza panel.jchost.pl lub na inny rachunek bankowy niż wskazany w proformie jest próbą oszustwa.
3. Nie prosimy o przesłanie hasła, kodu authinfo ani kodu jednorazowego – ani w wiadomości, ani telefonicznie. Nie wysyłamy załączników wykonywalnych ani archiwów z „fakturami".
4. Wiadomości weryfikacyjne dotyczące danych abonenta domeny zawierają odnośnik lub kod do potwierdzenia w Panelu Klienta; jeżeli masz wątpliwości, potwierdź dane bezpośrednio po zalogowaniu do panel.jchost.pl albo skontaktuj się z nami pod numerem telefonu podanym na stronie https://jchost.pl/kontakt/.
5. Podejrzaną wiadomość podszywającą się pod JCHost.pl prześlij nam w załączniku (najlepiej jako plik .eml lub z pełnymi nagłówkami) na adres biuro@jchost.pl – pomoże nam to ostrzec innych klientów i zablokować kampanię.

5) ZGŁOŚ CYBERZAGROŻENIE, INCYDENT LUB PODATNOŚĆ

1. Każdy użytkownik naszych usług – klient, użytkownik jego strony lub poczty, badacz bezpieczeństwa – może zgłosić nam:

    a. **cyberzagrożenie** – potencjalną okoliczność, zdarzenie lub działanie, które może wyrządzić szkodę lub zakłócić działanie usług (na przykład kampanię phishingową podszywającą się pod JCHost.pl albo stronę phishingową utrzymywaną na naszym hostingu);
    b. **incydent** – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów (na przykład włamanie na stronę lub skrzynkę, wyciek danych, rozsyłanie spamu lub złośliwego oprogramowania z naszej infrastruktury, atak na serwer);
    c. **podatność** – słabość produktu lub usługi, która może zostać wykorzystana przez cyberzagrożenie (na przykład błąd w Panelu Klienta, w konfiguracji serwera pocztowego albo w oprogramowaniu udostępnianym w ramach usług).

2. Zgłoszenie możesz przekazać:

    a. przez formularz zgłoszeniowy „Zgłoś nadużycie/Report abuse (Punkt kontaktowy)" – dział „Dział nadużyć (ABUSE)": https://panel.jchost.pl/submitticket.php?step=2&deptid=4&subject=Zg%C5%82oszenie%20cyberzagro%C5%BCenia%20%2F%20incydentu%20%2F%20podatno%C5%9Bci (formularz jest dostępny także bez logowania);
    b. pocztą elektroniczną na adres biuro@jchost.pl;
    c. w sprawach pilnych, dotyczących trwającego ataku lub niedostępności usług – dodatkowo telefonicznie pod numerami podanymi na stronie https://jchost.pl/kontakt/.

3. W zgłoszeniu podaj: czego dotyczy (adres strony, domena, nazwa usługi), na czym polega problem i kiedy go zauważyłeś, w miarę możliwości zrzuty ekranu, pełne nagłówki wiadomości lub fragmenty logów oraz dane kontaktowe, jeżeli oczekujesz informacji zwrotnej. Nie przesyłaj w zgłoszeniu haseł ani innych danych dostępowych.
4. Co dzieje się ze zgłoszeniem: potwierdzamy jego przyjęcie, analizujemy je i podejmujemy działania odpowiednie do wagi zagrożenia – na przykład zabezpieczenie usługi, kontakt z klientem, którego usługi dotyczy zgłoszenie, usunięcie nielegalnych treści, zgłoszenie incydentu poważnego do właściwego zespołu CSIRT. O wyniku informujemy zgłaszającego, o ile podał dane kontaktowe i pozwalają na to przepisy prawa. Dane zgłaszającego wykorzystujemy wyłącznie do obsługi zgłoszenia, na zasadach opisanych w naszej polityce prywatności.

§

5. Zgłoszenie podatności traktujemy jako działanie w dobrej wierze, jeżeli zgłaszający nie wykorzystuje wykrytej podatności ponad zakres niezbędny do jej wykazania, nie uzyskuje dostępu do cudzych danych ani ich nie kopiuje oraz powstrzymuje się od publikowania informacji o podatności do czasu jej usunięcia.
6. Zgłoszenia dotyczące nielegalnych treści na stronach naszych klientów rozpatrujemy w trybie Aktu o usługach cyfrowych opisanym w pkt 13 regulaminu serwisu, przez ten sam formularz. Reklamacje dotyczące usług składa się w trybie opisanym w pkt 18 regulaminu serwisu.

6) JAK INFORMUJEMY O POWAŻNYCH ZAGROŻENIACH I INCYDENTACH

1. Jeżeli dowiemy się o poważnym cyberzagrożeniu, które może mieć wpływ na Twoje usługi, poinformujemy Cię o możliwych środkach zapobiegawczych, a o samym zagrożeniu – jeżeli nie zwiększy to ryzyka dla bezpieczeństwa systemów. O incydencie poważnym, który ma niekorzystny wpływ na świadczenie usług, informujemy użytkowników usług, których incydent dotyczy.
2. Komunikaty przekazujemy na adres e-mail podany w Panelu Klienta, w Panelu Klienta oraz – w przypadku zdarzeń dotyczących wielu klientów – na stronie JCHost.pl. Dlatego ważne jest, aby Twój adres e-mail w Panelu Klienta był aktualny.

7) GDZIE SZUKAĆ DALSZYCH INFORMACJI

1. CERT Polska (CSIRT NASK) – krajowy zespół reagowania na incydenty: https://cert.pl/ – aktualne ostrzeżenia, analizy i porady bezpieczeństwa.
2. Zgłoszenie incydentu do CERT Polska: https://incydent.cert.pl/ – zgłoszenie do zespołu krajowego nie zastępuje zgłoszenia do nas, ale jest wskazane w przypadku oszustw, phishingu i innych zdarzeń wykraczających poza nasze usługi.
3. Lista ostrzeżeń CERT Polska przed niebezpiecznymi stronami: https://cert.pl/lista-ostrzezen/.
4. Baza wiedzy o cyberbezpieczeństwie Ministerstwa Cyfryzacji – porady dla każdego i dla firm: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo.
5. CSIRT GOV – zespół reagowania na incydenty w administracji rządowej: https://csirt.gov.pl/.
6. Rejestr domeny .pl (NASK) – bezpieczeństwo domeny i nowe obowiązki abonentów: https://www.dns.pl/bezpieczenstwo_domeny_pl oraz https://www.dns.pl/KSC_FAQ.

8) PODSTAWA PRAWNA

1. Informacje na tej stronie udostępniamy na podstawie art. 9 ust. 1 pkt 2 i 3 oraz art. 9 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2026 r. poz. 20 z późn. zm.), wdrażającej dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS 2). Zasady informowania o poważnych cyberzagrożeniach i incydentach wynikają z art. 11 ust. 2a i 2b tej ustawy. Pojęcia cyberzagrożenia, incydentu i podatności rozumiemy zgodnie z art. 2 pkt 4a, 5 i 11 ustawy oraz art. 2 pkt 8 rozporządzenia (UE) 2019/881.