Warszawa, dnia 15 września 2020 r.

Naukowa i Akademicka Sieć Komputerowa -
Państwowy Instytut Badawczy
CSIRT NASK
ul. Kolska 12
01-045 Warszawa

Raport z badania bezpieczeństwa strony www.zs-biala.idsl.pl

Jesteśmy zespołem reagowania na incydenty naruszenia bezpieczeństwa informatycznego w CERT Polska. Zespołowi CERT Polska zostały powierzone obowiązki CSIRT NASK wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560). Jednym z nich jest opieka nad placówkami oświatowymi. W przypadku wystąpienia incydentu bezpieczeństwa informatycznego, można go zgłosić za pomocą formularza dostępnego na stronie https://incydent.cert.pl.

W okresie od czerwca do sierpnia 2020r. zespół CERT Polska przeprowadził nieinwazyjne badania na stronach placówek oświatowych, których celem było sprawdzenie ich stanu bezpieczeństwa. Niniejszy raport stanowi podsumowanie błędów i złych praktyk wykrytych na stronie:
www.zs-biala.idsl.pl.
Jednocześnie informujemy, że dodatkowym podsumowaniem badań będzie zbiorczy zanonimizowany raport dla wszystkich przebadanych placówek oświatowych.

Wykryte podatności i złe praktyki:

HTTPS

W polu CN certyfikatu TLS wykorzystywanego przez stronę www.zs-biala.idsl.pl widnieje domena idsl.pl. Z tego powodu serwer nie obsługuje poprawnie protokołu HTTPS. Rekomendujemy wgranie certyfikatu z polem CN zgadzającym się z domeną na której jest wykorzystywany.

Błędy w konfiguracji domeny

Poniżej znajdują się wykryte błędy dotyczące konfiguracji domeny.

SPF

Serwer posiada rekord MX oznaczający możliwość obierania poczty e-mail, ale nie posiada rekordu SPF (Sender Policy Framework). Jest to mechanizm pozwalający na weryfikację przez serwery odbierające

pocztę z adresem "koperty" (envelope sender) w Państwa domenie czy wiadomość została faktycznie wysłana z Państwa serwerów.

Podstawowe porady

Z przeprowadzonych badań wyłonił się szereg problemów mogących mieć wpływ na cyberbezpieczeństwo stron instytucji oświatowych. Na podstawie zgromadzonych wyników ze wszystkich badanych instytucji wyciągnięto wnioski oraz ustalono zestaw porad ułatwiających kontrolowanie bezpieczeństwa systemów. Poniżej przedstawiamy podstawowe rekomendacje, które pozwalają niskim nakładem pracy wyeliminować większość z napotkanych problemów.

1. Regularnie aktualizować systemy zarządzania treścią, ich wtyczki oraz skórki. Jeśli strona nie jest oparta o tego typu system, aktualizować jej komponenty, jak np. biblioteki javascript.
2. Zadbać o poprawne wystawienie i ważność certyfikatów. Konfigurować automatyczne przekierowanie strony z protokołu http na https.
3. Zwracać szczególną uwagę na pliki wystawione publicznie (przez serwer HTTP czy FTP), zwłaszcza na to, czy nie zawierają wrażliwych informacji, takich jak dane osobowe czy dane logowania.
4. Zapewnić odpowiednią izolację usług od Internetu i nie pozwalać na dostęp z zewnątrz do usług, do których nie jest to niezbędne (np. baz danych).
5. Uczulić wszystkie osoby, mające dostęp do wprowadzania zmian na stronie, na używanie silnych haseł.
6. Zadbać o poprawność i aktualność danych w rejestrze domen.