NASK
CERT.PL

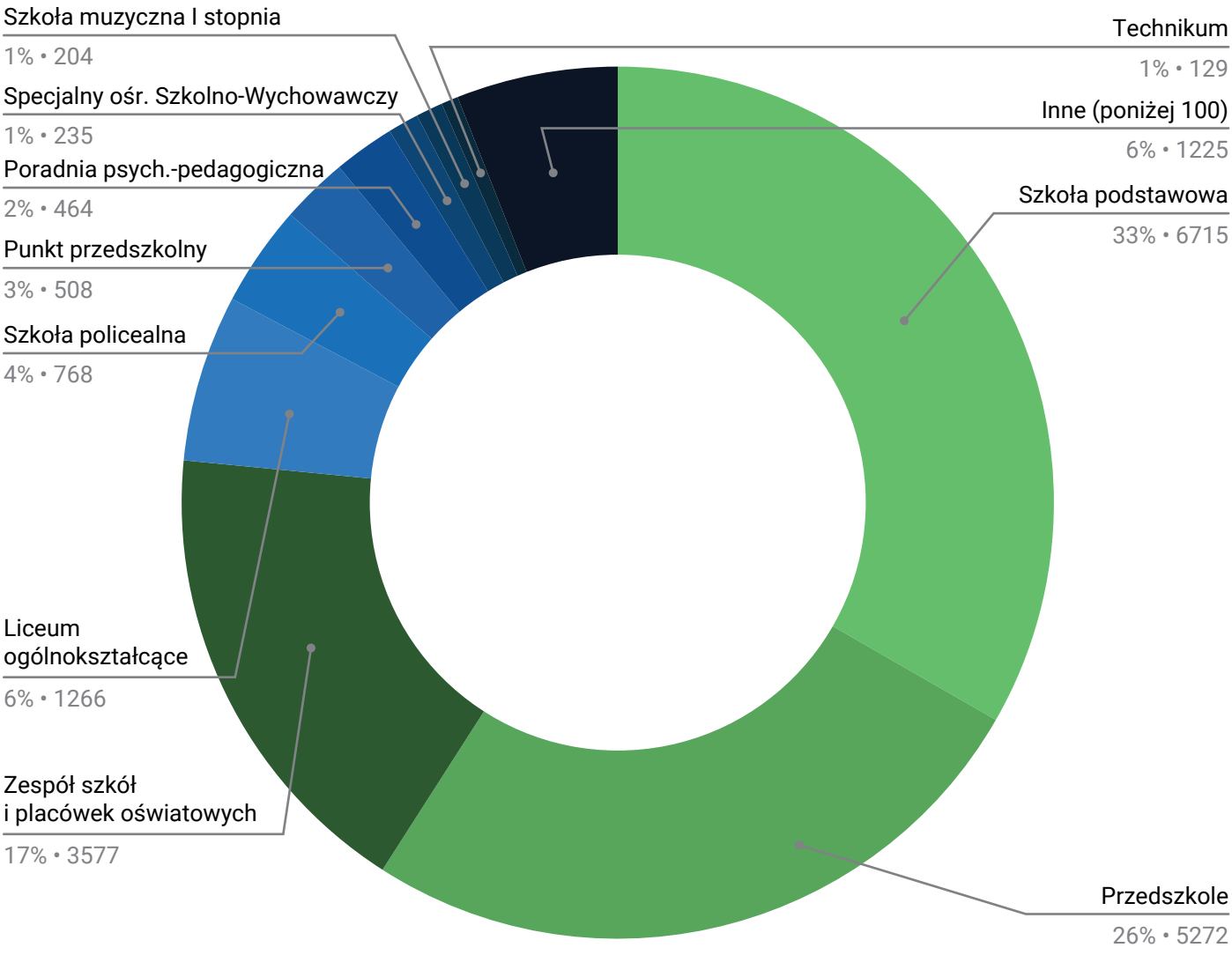
Raport dotyczący stanu bezpieczeństwa stron placówek oświatowych w Polsce

Wstęp

Opis badania

CERT Polska realizując niniejsze działanie kierował się obowiązkami nałożonymi Ustawą o Krajowym Systemie Cyberbezpieczeństwa[1], a w szczególności zadaniami opisanymi w rozdziale 6 Art. 26 Pkt. 3. Badanie bezpieczeństwa stron placówek oświatowych zostało przeprowadzone przez ekspertów zespołu CERT Polska między 19 czerwca a 15 sierpnia 2020. Do badania wykorzystano dane z **wykazu szkół i placówek oświatowych** (stan z 20 maja 2020)[2]. W wykazie znajduje się 34920 rekordów, z czego 22396 posiadało podaną stronę internetową – część placówek nie posiada lub nie zgłosiła swojej strony internetowej. W momencie prowadzenia badania 1932 z tych stron było nieosiągalnych. Finalnie badaniu zostały poddane 20464 adresy internetowe, stanowiące **17911 unikalnych domen** oraz **6602 unikalne adresy IP**, na które te domeny wskazywały. Rozkład typów placówek oświatowych, których strony zostały poddane badaniu, przedstawiono na rys. 1, 72% z nich stanowiły placówki publiczne.

Rys. 1. Rozkład typów placówek oświatowych poddanych badaniu



1 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz.U. 2018 poz. 1560

2 https://dane.gov.pl/dataset/839,wykaz-szko-i-placowek-oswiatowych/resource/23845/table

Zakres badania

W badaniu sprawdzono następujące aspekty:

- Analiza danych rejestrowych
- Czy strona jest hostowana na serwerze wspólnie ze stronami innych placówek oświatowych
- Otwarte porty i działające na nich usługi
- Wykorzystywane systemy zarządzania treścią (CMS)
- Znane podatności w wykorzystywanych wersjach systemu zarządzania treścią (Joomla, Wordpress)
- Wyszukiwanie ścieżek i plików w tzw. głębokim ukryciu, np. plików z kopią zapasową, plików konfiguracyjnych czy folderów z włączonym listingiem plików
- Podatności w usługach działających na serwerze
- Obecność i poprawność konfiguracji certyfikatów TLS
- Poprawność konfiguracji baz MySQL
- Poprawność konfiguracji FTP
- Poprawność konfiguracji serwerów pocztowych
- Poprawność konfiguracji DNS

W trakcie badania zespół CERT Polska zarejestrował **44 039 poważnych błędów**[3], które mogły skutkować krytycznymi problemami bezpieczeczeństwa, takimi jak utrata poufności lub dostępności. Informacja o wykrytych podatnościach wraz z niezbędnymi rekomendacjami została przekazana administratorom danych stron.

Dane statystyczne

Analiza domen

Analizie danych poddano 22354 nieunikalne, poprawne nazwy domenowe po wstępnej weryfikacji ich poprawności. Większość z nich (18642) to domeny krajowe - .pl, z czego 3169 to nazwy w domenach funkcjonalnych (w tym 2272 w nazwie .edu.pl), a 1808 w domenach regionalnych. Wśród przestrzeni nazw niebędących domenami funkcjonalnymi ani regionalnymi przodują "edupage.org", "szkolnastrona.pl" oraz "superszkolna.pl". Szczegółowe statystyki wykorzystywanych domen przedstawiono w tabelach 1, 2, 3.

Tabela 1. Najpopularniejsze domeny najwyższego poziomu (TLD)

pl	18642
org	1979
eu	601
com	547
net	379
info	125

Tabela 2. Najpopularniejsze polskie nazwy regionalne

waw.pl	231
gdansk.pl	161
krakow.pl	129
szczecin.pl	112
lublin.pl	94
bialystok.pl	88
wroclaw.pl	84
poznan.pl	78
olsztyn.pl	75
opole.pl	74
lodz.pl	70
wroc.pl	66
lublin.eu	51
radom.pl	50
zgora.pl	49
kalisz.pl	44
rzeszow.pl	39

3 Common Vulnerability Scoring System HIGH i CRITICAL

Tabela 3. Najpopularniejsze nazwy funkcjonalne oraz dostawców wspólnych usług

edu.pl	2272
edupage.org	1787
szkolnastrona.pl	1430
com.pl	459
superszkolna.pl	219
wikom.pl	204
szkolna.net	186
org.pl	162
net.pl	150
cba.pl	136
teb.pl	115

Analiza danych z rejestru domen

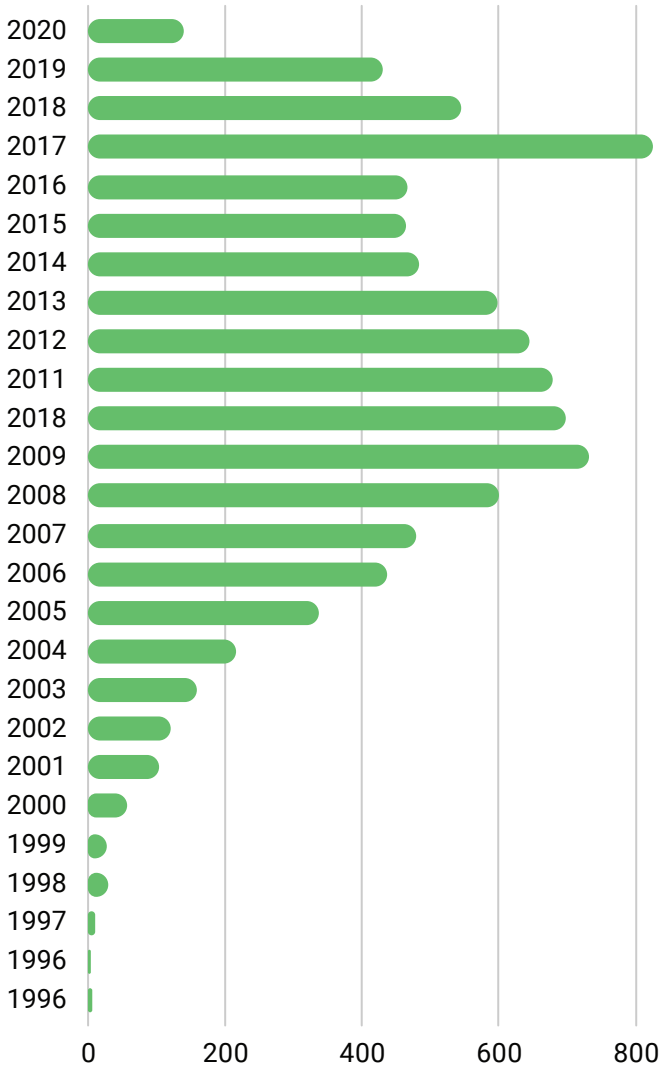
Analizie poddano dane rejestrowe przynależne do **9294 nazw domenowych**, które przekazywane są do rejestru .pl w momencie ich rejestracji. Rekomendowane jest aby domeny podmiotów takie jak szkoły i placówki oświatowe **rejestrowane były na dane tego podmiotu oraz wskazane były poprawne dane kontaktowe**. W przypadku gdy domena zarejestrowana została na osobę prywatną, stwarza to zagrożenie w postaci trudności w odnowieniu ważności rejestracji albo w ewentualnych postępowaniach spornych przed Sądem Polubownym bądź Arbitrażowym, co ostatecznie skończyć się może utratą kontroli nad nazwą domenową. Może dojść do takich sytuacji zwłaszcza wtedy, gdy osoba, na której dane zarejestrowana jest domena zakończy swój stosunek pracy ze szkołą, jednostką samorządu prowadzącego placówkę oświatową albo wygaśnie umowa z osobą będącą podwykonawcą, który zarządza stroną internetową.

Spośród wszystkich 9294 przeanalizowanych domen, **1090 było zarejestrowanych na osobę prywatną**. Natomiast w przypadku aż **4379 domen skrzynka pocztowa podana jako kontakt była darmową usługą** (gmail.com, wp.pl, o2.pl, onet.pl, interia.pl, poczta.fm, tlen.pl czy gazeta.pl). W przypadku 1181 domen, skrzynka pocztowa podana w danych kontaktowych była zgodna z zarejestrowaną domeną.

Dane kontaktowe w **postaci numeru telefonu lub faksu podano w 5256 przypadkach**. Jest to opcjonalne, natomiast rekomendowane, ponieważ ułatwia kontakt z rejestratorem, rejestrem czy innymi uprawnionymi organami w sprawach związanych m.in. z prowadzeniem przez szkołę i jednostki oświatowe ich stron internetowych.

Przeanalizowano również datę oryginalnej rejestracji każdej z domen. Rozkład lat rejestracji przedstawiono na rys. 2. Zwiększona liczba rejestracji w 2017 związana jest najprawdopodobniej z przeprowadzoną w tym roku reformą struktury szkolnictwa.

Rys. 2. Rozkład lat rejestracji domen szkół i jednostek oświatowych



Wykorzystywane serwery

Utrzymywanie wielu stron na jednym serwerze nie jest podatnością samą w sobie, jednak poważnie zwiększa ryzyko ataku, np. w wyniku przejęcia serwera poprzez błędy w innych witrynach lub wyciek wrażliwych danych do osób zarządzających innymi serwisami przez błędną konfigurację serwera.

Bardzo często strony szkół korzystają z gotowych rozwiązań dedykowanych dla szkół, utrzymywanych w obrębie jednego dostawcy. Widoczne to jest już po analizie rozszerzeń domen, gdzie popularne są subdomeny w obrębie domen edupage.org, szkolnastrona.pl czy superszkolna.pl. Z jednej strony stanowi to ryzyko, ale z drugiej, w momencie, gdy wszystkie usługi na serwerze są na bieżąco aktualizowane, a strona ma jedynie formę reprezentacyjną, taka scentralizowana forma może przynieść korzyści. W badaniu sprawdzono skalę tego zjawiska. Wyniki dla 10 najczęściej wykorzystywanych adresów IP przedstawiono w tab. 4.

Tabela 4. Serwery hostujące największą liczbę stron placówek oświatowych

Adres IP	Liczba stron szkół	Dostawca usług wspólnych
Adres 1	593	edupage.org
Adres 2	370	edupage.org
Adres 3	331	szkolnastrona.pl
Adres 4	317	superszkolna.pl
Adres 5	286	szkolnastrona.pl
Adres 6	260	edupage.org
Adres 7	239	edupage.org
Adres 8	215	szkolnastrona.pl
Adres 9	180	szkolnastrona.pl
Adres 10	139	wikom.pl

Otwarte porty

W ramach badania przeskanowano otwarte porty na serwerach hostujących strony placówek oświatowych. W tab. 5 prezentujemy najczęściej otwarte porty, czyli takie, które zostały wykryte na przynajmniej 500 hostach. Część z tych usług została dokładniej zbadana w kolejnych rozdziałach. W tabeli nie uwzględniono portów 80 i 443, potrzebnych do działania strony WWW i dostępnych na każdym z badanych hostów.

Tabela 5. Najczęściej występujące otwarte porty na przebadanych hostach

Numer portu	Liczba serwerów, na których wykryto port jako otwarty	Usługa prawdopodobnie działająca na porcie
21	4795	ftp
587	4368	smtp
25	4355	smtp
993	4329	imap (ssl)
995	4326	pop3 (ssl)
110	4305	pop3
143	4266	imap
465	4265	smtp (ssl)
3306	3927	mysql
5432	3057	postgresql
22	1892	ssh
1433	1531	mssql
53	1273	dns

Systemy zarządzania treścią

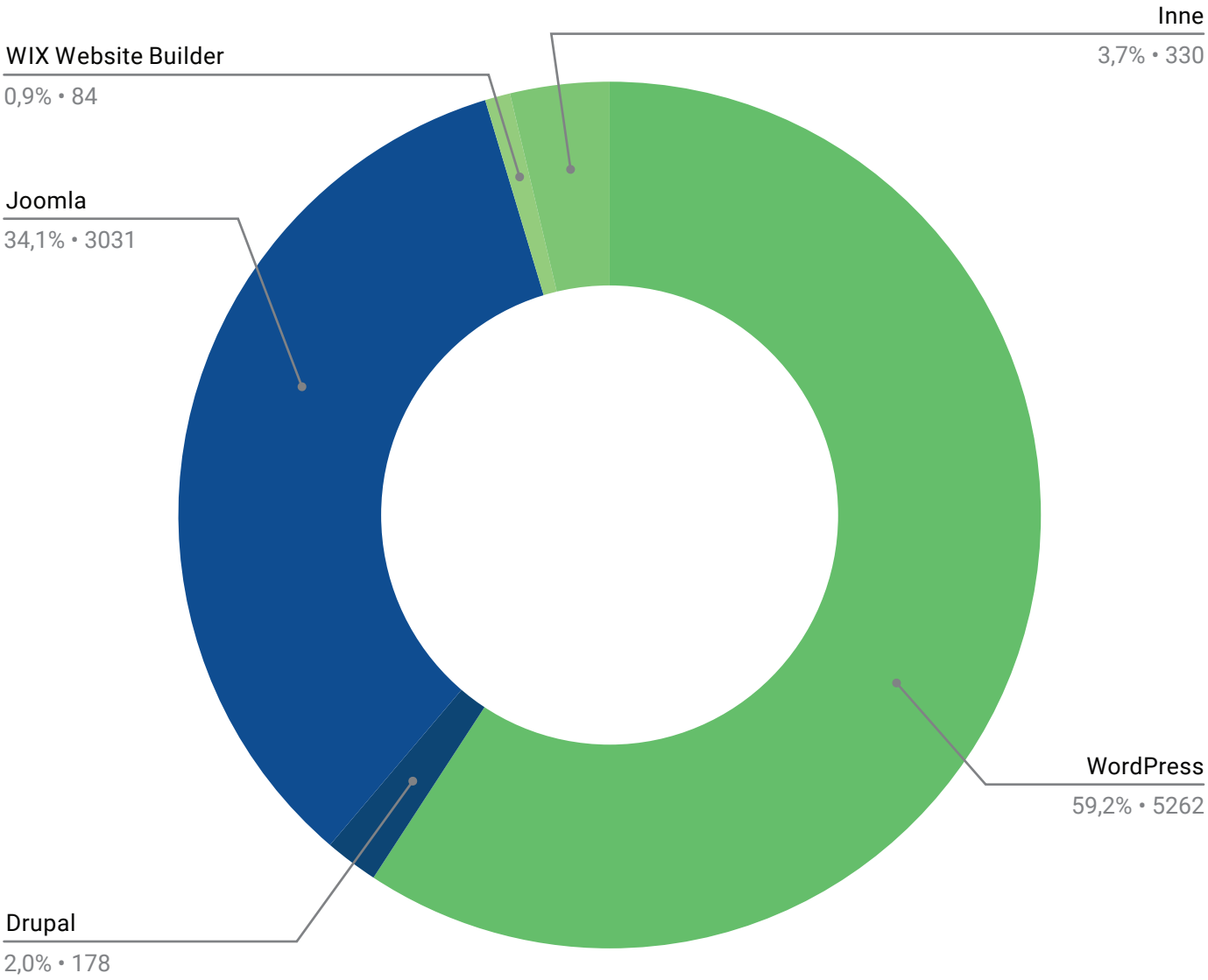
Częstą praktyką przy tworzeniu stron jest korzystanie z gotowych systemów zarządzania treścią (CMS). Samo w sobie nie jest to groźne, o ile dany system oraz wszystkie jego komponenty utrzymywane są w najnowszej wersji. Niestety często zdarza się, że tego typu systemy po pierwszym zainstalowaniu nie są dalej utrzymywane.

W przypadku stron placówek oświatowych **znany system zarządzania treścią udało się wykryć w 8885 przypadkach (43%)**. Najczęściej był to WordPress[4] oraz Joomla[5], dlatego właśnie te systemy wybrano do dokładniejszego

4 https://wordpress.org/
5 https://www.joomla.org/

badania opisanego w dalszych rozdziałach. Rozkład rozpoznanych systemów przedstawiono na rys. 3.

Rys. 3. Rozkład rozpoznanych systemów zarządzania treścią na stronach polskich placówek oświatowych



Wyniki szczegółowych badań

Testowanie bezpieczeństwa stron opartych o CMS Joomla

Zespół CERT Polska przeskanował strony placówek oświatowych narzędziem joomscan. Udało się uzyskać wynik dla 2873 stron z systemem Joomla, na których **łącznie znaleziono 5175 podatności**.

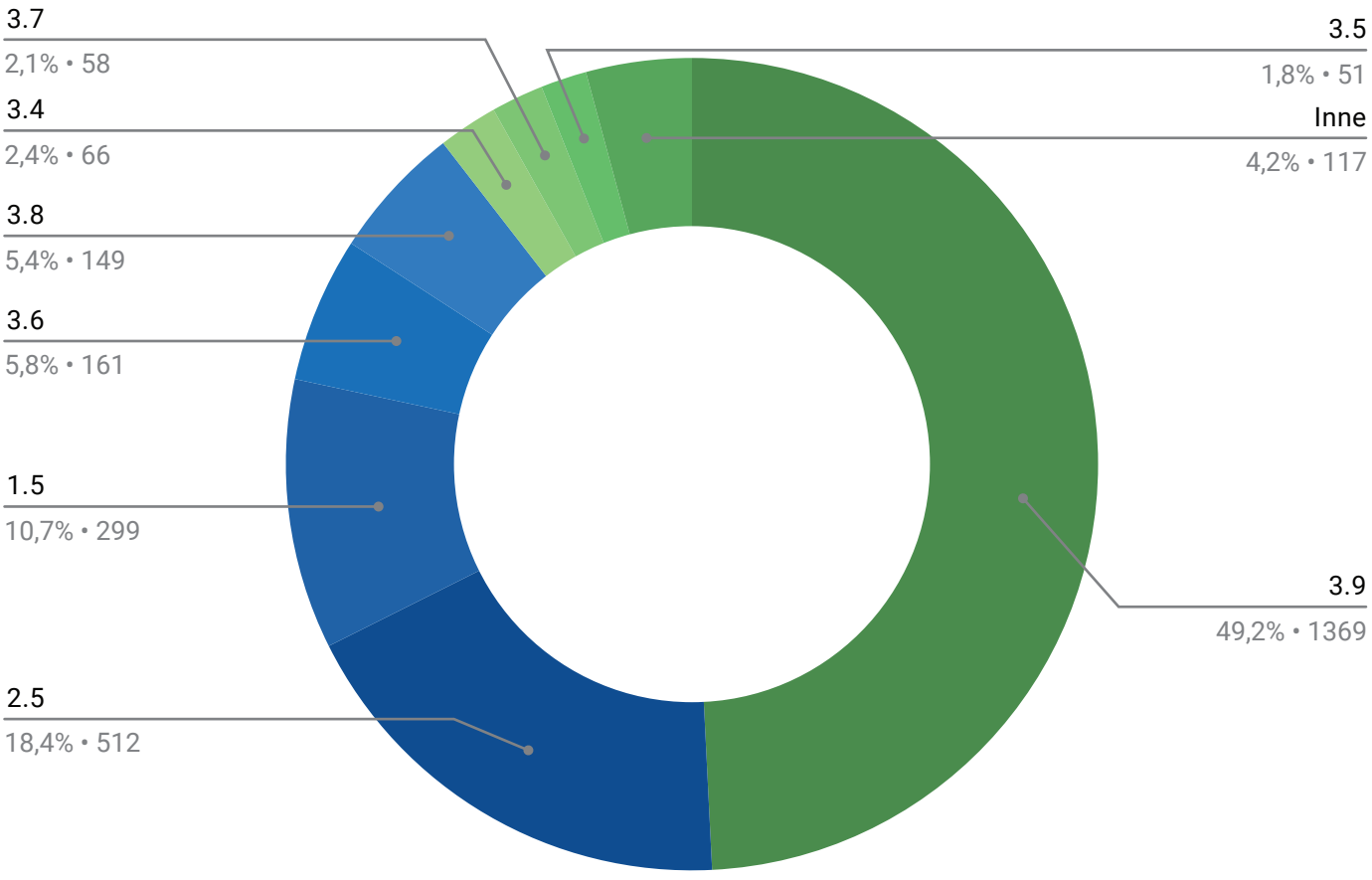
Częstym przypadkiem były strony posiadające wiele podatności, głównie z uwagi na wykorzystanie starej wersji Joomli, czy jej pluginów, co znacznie zawyża łączną liczbę błędów na wszystkich stronach. W przypadku gdy spojrzymy tylko na unikalne strony, to **na 827 stronach (25%) znajdowała się przynajmniej jedna podatność o klasyfikacji wysokiej**.

Tę liczbę można przyjąć jako szacunkową, określającą procent stron placówek oświatowych, korzystających z systemu Joomla, podatnych na atak, który może być dotkliwy w skutkach.

Błędy o klasyfikacji wysokiej najczęściej dotyczyły podatności typu SQL Injection, Directory Traversal, czy pozwalających na zdalne wykonanie kodu na serwerze (RCE). Występowanie takich podatności pozwala atakującemu na wykradanie danych z bazy (w tym danych logowania do panelu administracyjnego), przeglądania wewnętrznych plików witryny czy nawet przejęcia całkowitej kontroli nad serwerem.

Dokładny rozkład wykorzystywanych wersji systemu Joomla na przebadanych stronach przedstawiono na rys. 4. Należy zauważyć, że prawie połowa stron (49,2%) korzystała z najnowszej dostępnej wersji 3.9, co świadczy o regularnie dokonywanych aktualizacjach. Jednak część ze sprawdzonych instancji posiadała bardzo starą wersję systemu, co może stanowić łatwy cel dla atakujących.

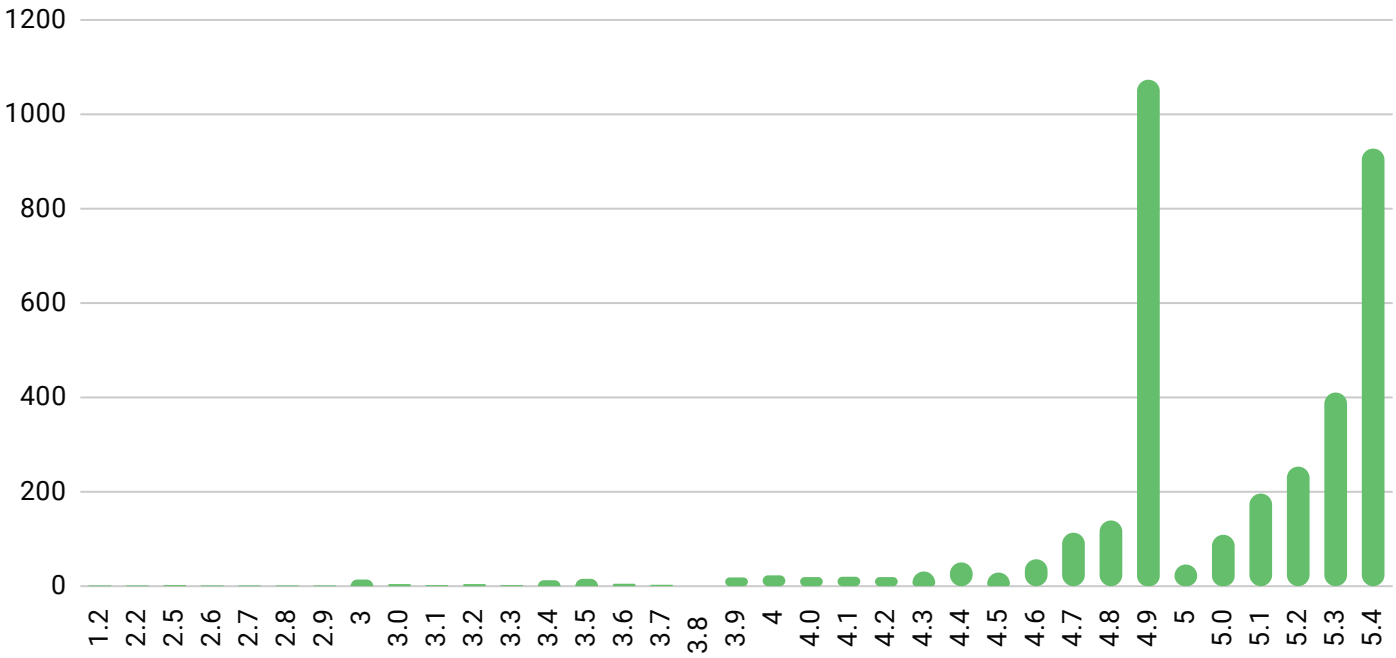
Rys. 4. Wykorzystywane wersje Joomli



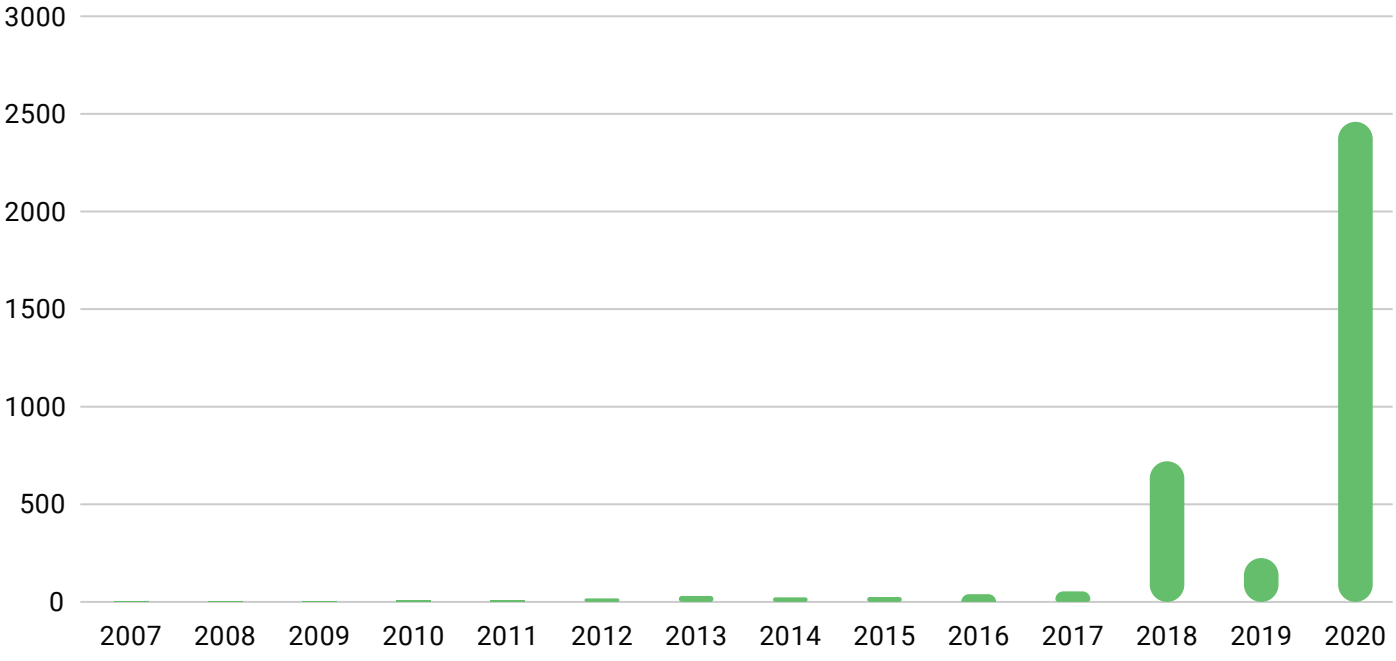
Testowanie stron opartych o CMS WordPress

6602 strony zostały zidentyfikowane jako oparte na systemie zarządzania treścią WordPress. Zostały one przeskanowane narzędziem wpscan. Rozkład wykorzystywanych wersji systemu przedstawiono na rys. 5. Niemal połowa stron korzystała z CMS-a w najnowszej wersji, co świadczy o regularnych aktualizacjach. Z uwagi, że Wordpress posiada kilka głównych gałęzi rozwoju i w czasie badania zarówno wersja 4.9, jak i 5.4 były najnowszymi, na rys. 6 przedstawiono rok ostatniej aktualizacji, w celu lepszej reprezentacji częstotliwości dokonywania aktualizacji.

Rys. 5. Wykorzystywane wersje systemu WordPress



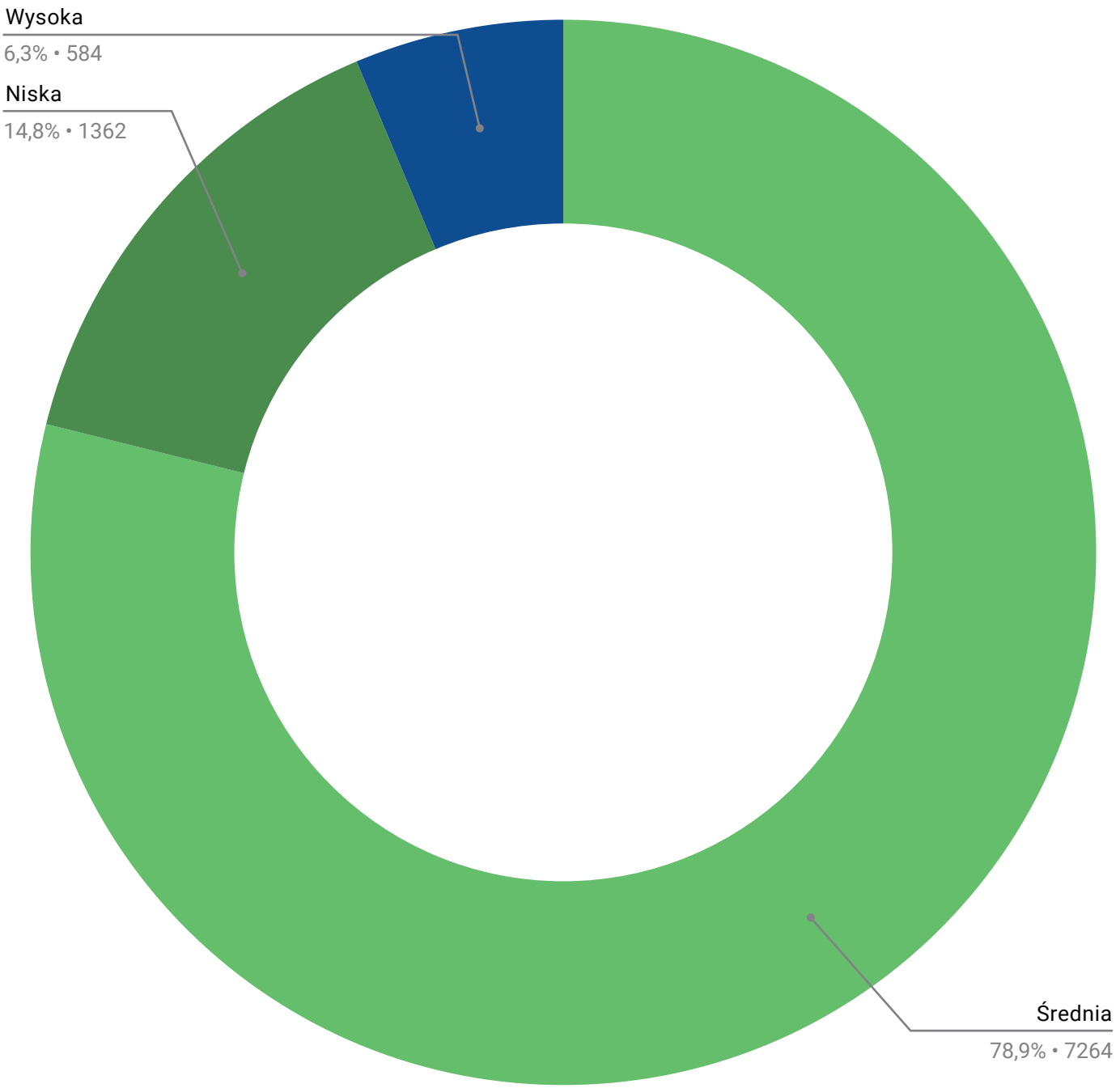
Rys. 6. Rok ostatniej aktualizacji znalezionych systemów WordPress



Spośród 6602 sprawdzonych stron, **1134 strony miały co najmniej jedną podatność**, 1048 co najmniej jedną podatność poza tymi o niskiej krytyczności, oraz **264 podatności o klasyfikacji wysokiej**. Zazwyczaj było to związane z wykorzystaniem starej wersji WordPressa. Łącznie odnalezionych zostało 9210 podatności na wszystkich sprawdzonych stronach – zarówno w samym systemie zarządzania treścią, jak i w pluginach. Rozkład krytyczności tych podatności przedstawiono na rys. 7. Co najmniej 92 podatności zostały zaklasyfikowane jako RCE, 991 jako SQLI, a 4234 jako XSS.

Dodatkowo dla stron opartych na WordPressie przeprowadzone zostało sprawdzenie paneli administracyjnych pod kątem użycia słabych haseł (zawierających nazwę szkoły czy popularne słowa typu “admin”, lub “hasło”). Dostęp do panelu administracyjnego udało się uzyskać w ten sposób w jednym przypadku.

Rys. 7. Rozkład krytyczności podatności znalezionych na stronach z systemem WordPress



Poufne pliki dostępne na stronach

Wszystkie strony placówek oświatowych zostały zeskanowane przy użyciu narzędzia meg[6] z odpowiednio skonstruowanym słownikiem. Celem badania było wykrycie kopii zapasowych, plików konfiguracyjnych oraz folderów z włączonym listingiem plików, które można było przeglądać z powodu błędnej konfiguracji serwera.

W kilkudziesięciu przypadkach znaleziono katalogi, które posiadały włączony listing plików, tzw. open directory. W większości foldery te zawierały wewnętrzne pliki serwisu, lecz dostęp do nich nie powodował negatywnych konsekwencji dla placówki oświatowej (np. galeria zdjęć i tak wyświetlana na stronie głównej). **W pojedynczych przypadkach udało się jednak trafić na dane wrażliwe, jak kopie zapasowe czy logi, które powinny być niejawne**.

W 6 przypadkach znaleziono archiwa zawierające kopie całej strony wraz z plikami konfiguracyjnymi, a w 11 kopie bazy danych. Pliki te były dostępne do pobrania bez żadnych zabezpieczeń, a jedynym utrudnieniem było poznanie odpowiedniego adresu. Najczęściej były to pliki o oczywistym nazewnictwie jak backup.sql czy web.tar.gz.

W przypadku znacznej części szkół badanie dostępnych ścieżek ujawniło publiczny dostęp do panelu administracyjnego CMS-a lub bazy danych (np. phpmyadmin). Samo w sobie nie jest to traktowane jako podatność, ale znacznie zwiększa powierzchnię ataku oraz ułatwia eskalację, np. w przypadku uzyskania poświadczeń administracyjnych.

Podatności na serwerach hostujących strony

W ramach badania pobrano dane o podatnościach na badanych hostach (6602 adresy IP) z bazy wyszukiwarki Shodan. Głównie są to podatności, które da się rozpoznać w sposób nieinwazyjny - po danych z bannerów czy nagłówków zwracanych przez serwery, np. podatności związane ze starą wersją Apache czy PHP.

Na 3137 hostach (47%) znaleziono przynajmniej jedną podatność. Łącznie hosty te posiadały 63311 podatności zawierających się w 1081 różnych CVE. W tabeli 6 przedstawiono top 20 najczęściej występujących podatności. W 16 przypadkach znaleziono ponad 100 różnych podatności na jednym serwerze.

Tabela 6. Top 20 podatności znalezionych na hostach wg. wyszukiwarki Shodan

CVE	Liczba wystąpień
CVE-2018-1115	1916
CVE-2017-7486	1915
CVE-2017-12172	1909
CVE-2017-15098	1909
CVE-2017-7546	1907
CVE-2018-1058	1907
CVE-2017-7484	1907
CVE-2017-7485	1907
CVE-2019-9193	1907
CVE-2017-7547	1907
CVE-2016-5423	1848
CVE-2016-5424	1848
CVE-2017-7548	1004
CVE-2016-0773	945
CVE-2016-0766	945
CVE-2017-15099	941
CVE-2016-2193	939
CVE-2016-3065	939
CVE-2017-14798	918
CVE-2016-7048	912

W większości nie są to poważne podatności, ale wśród nich można znaleźć i krytyczne. Celem natychmiastowego powiadomienia dotkniętych podmiotów, wyróżniono taki katalog podatności krytycznych. Poprzez podatność krytyczną uznano taką, która nie wymaga wcześniejszych poświadczeń ani interakcji użytkownika, oraz daje możliwość zdalnego wykonania kodu. W trakcie badania znaleziono 31 podatnych serwerów, rozkład CVE przedstawiono w tabeli 7.

6 https://github.com/tomnomnom/meg

Tabela 7. Znalezione podatności krytyczne

CVE	Nazwa	Liczba wystąpień
CVE-2019-10149	Exim RCE	27
CVE-2020-1938	Tomcat RCE (ghostcat)	3
CVE-2019-0708	RDP RCE (bluekeep)	1

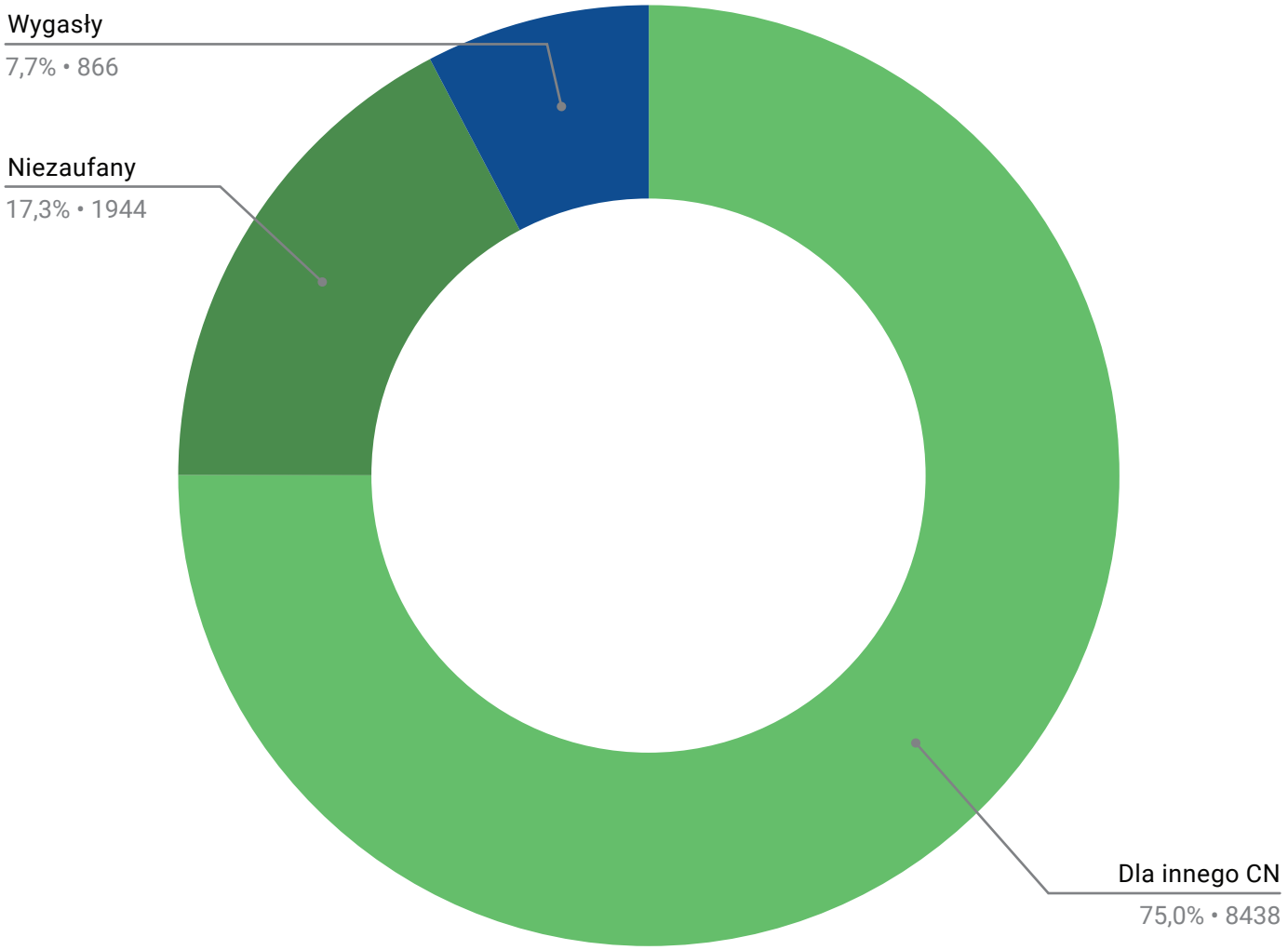
Bezpieczeństwo połączenia – certyfikaty TLS

W trakcie badania zespół CERT Polska sprawdził czy strony posiadają dobrze skonfigurowany, ważny certyfikat TLS oraz wymuszone przekierowanie z http na https.

Na 17911 przebadanych domen aż 16835 zwróciło jakiś certyfikat. Niestety ogromna część z nich była źle skonfigurowana. Wynika to głównie z tego, że często w domyślnej konfiguracji pod portem 443 strona zwraca certyfikat hostingodawcy. Świadczy o tym fakt, że niezgodność badanej domeny i nazwy CN w certyfikacie miała miejsce aż w **8438 przypadkach.** Bardzo często CN skonfigurowany był np. dla *.home.pl czy *.nazwa.pl.

W 866 przypadkach zwracany certyfikat był wygasły. Oznacza to, że został prawdopodobnie wgrany świadomie, ale został błędnie skonfigurowany. **W 1944 przypadkach** certyfikaty nie zostały podpisane przez zaufane centrum certyfikacji. Były to najczęściej tzw. certyfikaty self-signed. Wszystkie problemy z certyfikatami zobrazowano na rys. 8. W przypadku, gdy dana strona posiadała więcej niż jeden problem, na wykresie została ona uwzględniona w kilku obszarach.

Rys. 8. Główne zidentyfikowane problemy z certyfikatami



Sprawdzono też ile stron, z tych, które zwracają jakiś certyfikat, posiada skonfigurowane automatyczne **przekierowanie z http na https. Okazało się że takie przekierowanie jest skonfigurowane na 5679 przebadanych domenach**, co stanowi tylko 33% wszystkich stron, które zwróciły jakiś certyfikat.

Ostatecznie 7835 domen zwróciło w pełni poprawnie skonfigurowany certyfikat (44% badanych). Jeśli uwzględnimy również skonfigurowanie automatycznego przekierowania z http na https, to liczba poprawnych wyniesie 7536 (42% badanych). Te domeny należy uznać za takie, gdzie nie wykryto żadnych problemów z certyfikatem.

Podczas badania sprawdzono również występowanie podatności Heartbleed (CVE-2014-0160), związanej z błędem w bibliotece OpenSSL. Podatność wykryto na 4 różnych domenach, o czym właściciele zostali natychmiast powiadomieni.

Poprawność konfiguracji MySQL

Podczas badania przebadano 3927 publicznie dostępnych serwerów MySQL skonfigurowanych na serwerach hostujących strony placówek oświatowych.

Większość instancji, bo aż 3786, wspierało logowanie loginem i hasłem z dowolnego miejsca w internecie. Tylko 98 miało skonfigurowaną listę dozwolonych adresów IP, a pozostałe 43 odrzucały połączenie z innymi błędami.

W większości przypadków (2827 serwerów), serwer mysql nie widział prawdziwego IP łączącego się użytkownika, co może sugerować wirtualizację albo load balancing u większych dostawców usług hostingowych. Nie znając szczegółów infrastruktury ciężko jednoznacznie ocenić wpływ na bezpieczeństwo, ale prawdopodobnie znaczy to, że serwery SQL są izolowane od aplikacji co jest przykładem obrony warstwowej (defence in depth).

Podczas testów próbowano zalogować się do serwera za pomocą kombinacji trzech prostych kombinacji nazwy i hasła użytkownika. Nie udało się zalogować do ani jednego.

W znacznej większości przypadków baza danych była wykorzystywana tylko na potrzeby strony znajdującej się na tym samym serwerze. W takim przypadku dobre praktyki wskazują, że dostęp ze świata powinien zostać ograniczony. Taka konfiguracja przełożyłaby się na zmniejszenie powierzchni ataku.

Poprawność konfiguracji FTP

Podczas badania sprawdzono 4795 serwerów FTP dostępnych na serwerach hostujących strony placówek oświatowych. **Z tego aż 999 pozwalało na dostęp anonimowy albo za pomocą kombinacji ftp:ftp**. Co najmniej 145 serwerów FTP zawierało przynajmniej jeden plik. Trudno jednoznacznie stwierdzić na ile takie otwarte serwery są działaniami zamierzonymi (np. żeby użytkownicy mogli pobrać dokumenty związane z placówką oświatową), a na ile jest to błąd konfiguracji. W kilku przypadkach znaleziono pliki zawierające dane uważane za wrażliwe, takie jak hasła, czy dane osobowe.

W 5 przypadkach usługa FTP była skonfigurowana, ale nie działała poprawnie. Na 21 serwerach usługa FTP zwracała jedynie zaślepkę informacyjną, kierującą do usługi FTPS. Nie jest to groźne zachowanie, ale w celu zmniejszenia potencjalnej powierzchni ataku zaleca się wyłączanie takich usług.

Poprawność konfiguracji serwerów poczty

Badanie poprawności konfiguracji serwerów poczty dotyczyło możliwości ewentualnego podszywania się przez atakujących pod adresy pocztowe w domenie szkół i jednostek oświatowych. Podstawowymi mechanizmami obrony przed podszywaniem się są: Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) oraz Domain-based Message Authentication (DMARC).

SPF jest standardem opisującym format rekordu TXT przypisanego przez administratorów danej domeny, który poprzez określoną politykę określa z których serwerów można wysyłać pocztę z wartością “MAIL FROM”/“Return-Pa-

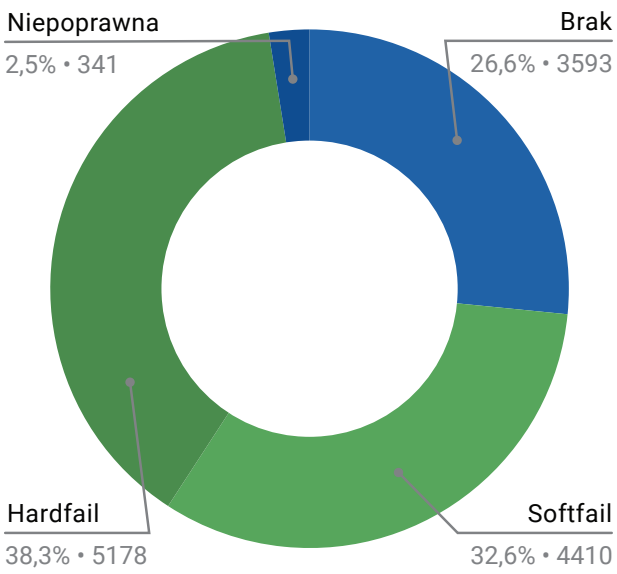
th"/"Envelope-Sender" w danej domenie. DKIM jest mechanizmem podpisywania wiadomości za pomocą kryptografii asymetrycznej. Klucze publiczne publikowane są jako rekordy TXT danej domeny. DMARC z kolei jest mechanizmem, który łączy weryfikację dwóch poprzednich mechanizmów z porównaniem domeny w nagłówku "From" oraz pozwala administratorowi domeny określić politykę ewentualnego odrzucenia wiadomości.

Każdy serwer odbierający pocztę na podstawie powyższych mechanizmów może sprawdzić czy nie doszło do przypadku wysłania wiadomości przez nieautoryzowany serwer i na tej podstawie odrzucić wiadomość, specjalnie ją oznaczyć albo umieścić w katalogu z wiadomościami o charakterze spamowym.

Z 22356 nazw domenowych szkół i jednostek oświatowych 13522 (60%) posiada rekord MX wskazujący na adres serwera, który może odebrać wiadomości email dla adresów w tej domenie. Dla wszystkich z nich dokonaliśmy bardziej szczegółowej analizy mechanizmu SPF. Aż **3593 domen z rekordem MX w ogóle nie posiada rekordu TXT z polityką SPF**, co pozwala dowolnym serwerom podszywać się pod domenę nadawcy w wartości "MAIL FROM". **233 domeny** posiadają politykę SPF **z kwalifikatorem neutralnym** dla każdego adresu ("?all"), a **108 domen nie posiada w ogóle mechanizmu** "all", "redirect" ani "include", co w obu przypadkach efektywnie oznacza brak polityki. Taki zapis powinien być używany tylko dla celów testowych. 4410 domen posiada politykę SPF z kwalifikatorem softfail dla każdego adresu ("~all"), co oznacza, że serwer nie daje jednoznacznej odpowiedzi na to czy dowolny serwer w internecie może wysyłać pocztę z tej domeny. Nie jest to błędem, jeżeli poprawnie wdrożone są dwa pozostałe mechanizmy – DKIM i DMARC.

Poprawnie zaimplementowany i skuteczny rekord SPF powinien na końcu zawierać regułę zabraniającą losowym serwerom na podszywanie się pod adresatów w naszej domenie, tj. "-all". W taki sposób skonstruowanych było 5178 sprawdzonych przez nas rekordów SPF. Statystyki polityk SPF badanych domen przedstawiono na rys 9.

Rys. 9. Polityki SPF badanych domen



Nie przeprowadzono analizy użycia DKIM przez serwery pocztowe szkół i jednostek oświatowych, ponieważ do jej wykonania potrzebne byłoby uzyskanie próbki treści wiadomości wysłanej z danego serwera wraz z jej nagłówkami.

Natomiast z **9929 domen posiadających politykę SPF tylko 1297 posiada również politykę DMARC**. Spośród nich, **546 nie posiada polityki "reject" lub "quarantine"**, co sprawia, że jest ona nieefektywna. Brak efektywnej polityki DMARC oznacza, że z dużym prawdopodobieństwem można podszyć się pod nadawcę nawet, gdy poprawnie skonfigurowany jest rekord SPF (ponieważ ten sprawdza wartość "MAIL FROM", a nie nagłówek "From" wyświetlany w klientach pocztowych).

Sprawdzono również jak wiele serwerów pocztowych szkół i jednostek oświatowych pozwala na **wysyłanie wiadomości email nieuwierzytelnionym użytkownikom** (czyli dowolnej osobie). Ponieważ nie istnieje prosty sposób na uzyskanie adresu takiego serwera, sprawdzenie przeprowadzono dla czterech wariantów adresu: domeny głównej, domeny z rekordu MX oraz z dodaniem nazwy "smtp." do dwóch poprzednich. Weryfikację przeprowadzono skryptem smtp-open-relay z pakietu nmap. W **15 przypadkach serwer pocztowy zwrócił informację o przyjęciu do wysyłki** testowej wiadomości email wysłanej bez wcześniejszego uwierzytelniania. Może to oznaczać, że te

serwery mogą być wykorzystane do wysyłania złośliwej poczty elektronicznej w imieniu szkoły lub jednostki oświatowej, np. o charakterze spamowej czy zawierającej załączniki ze złośliwym oprogramowaniem.

Podsumowując, z 13522 szkół i jednostek oświatowych, **aż 12771, tj. 94% nie posiada poprawnie skonfigurowanych mechanizmów** pozwalających na ochronę przed podszywaniem się pod adresy email w ich domenach. Przeanalizowane mechanizmy nie są jednak idealnym rozwiązaniem wszystkich problemów z bezpieczeństwem poczty elektronicznej. Nie są też zawsze skuteczne. Nie pokrywają również wszystkich przypadków używania poczty (np. przekierowywania poczty, grupowych aliasów czy list dyskusyjnych), dlatego nie zawsze mogą być w pełni wdrożone.

Poprawność konfiguracji serwerów DNS

Dla wszystkich nazw domenowych szkół i jednostek oświatowych na podstawie rekordu SOA zostały pobrane adresy ich serwerów autorytatywnych. Te serwery są w posiadaniu plików "stref" z listą wszystkich rekordów danej domeny włącznie z ich subdomenami. Następnie za pomocą protokołu AXFR odpytano każdy z nich o pełną kopię strefy. Poprawnie skonfigurowany serwer usługi DNS powinien pozwolić na wykonanie kopii tylko wcześniej zdefiniowanym i zaufanym adresom IP, np. dla celów replikacji. Mimo tego **udało się pomyślnie przeprowadzić transfery w 333 przypadkach**. W danych z transferu strefy atakujący mogą znaleźć informacje przydatne w fazie rekonesansu, np. listę wewnętrznych subdomen.

Warto podkreślić, że aż **170 z 333 transferów udało wykonać się z serwerów DNS tylko 12 firm** udostępniających szkołom i placówkom oświatowym usługi hostingu.

Rekomendacje

Z przeprowadzonych badań wyłonił się szereg problemów mogących mieć wpływ na cyberbezpieczeństwo stron placówek oświatowych. Poniżej przedstawiamy podstawowe rekomendacje, które pozwalają niskim nakładem pracy wyeliminować większość z napotkanych problemów.

CERT Polska zaleca:

- 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.
- Sprawdzić konfigurację i aktualność wykorzystywanych usług, w szczególności serwerów pocztowych i DNS.
- Zadbać o poprawne wystawienie i ważność certyfikatów. Konfigurować automatyczne przekierowanie strony z protokołu http na https.
- 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.
- Uczulić wszystkie osoby, mające dostęp do wprowadzania zmian na stronie, na używanie silnych haseł.
- Zapewnić odpowiednią izolację usług od Internetu i nie pozwalać na dostęp z zewnątrz do usług, do których nie jest to niezbędne (np. baz danych).
- Zadbać o poprawną konfigurację mechanizmów chroniących przed podszywaniem się pod domenę przy wysyłce maili (SPF, DMARC, DKIM).
- Zadbać o poprawność i aktualność danych w rejestrze domen.

Badanie wykonane w ramach zadań CSIRT NASK, sfinansowane częściowo w ramach dotacji podmiotowej z części budżetu państwa, której dysponentem jest minister właściwy do spraw informatyzacji, na podstawie art. 26 ust. 9 ustawy o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560)

NASK

CERT.PL