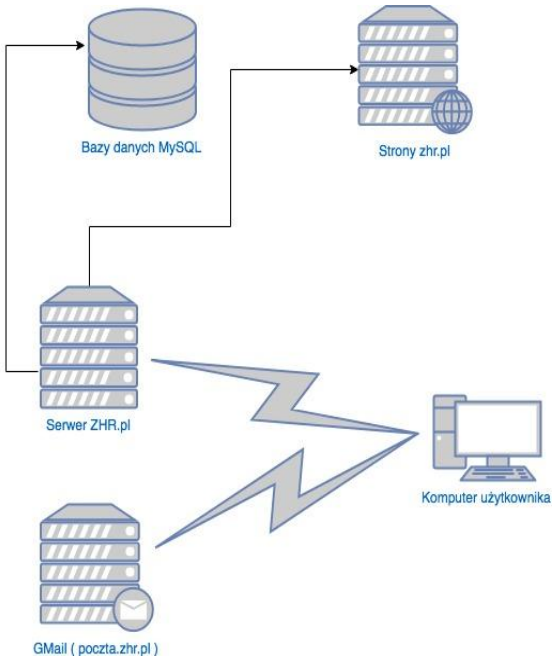
Sprawozdanie Zespołu MATRIX

oprac. przez phm. Adama Skarżyńskiego, ćw. Michała Kilijanka, phm. Marcina Stożka

1. Stara architektura zhr.pl

Dotychczasowa architektura przewidywała pojedynczy fizyczny serwer (hostujący strony www oraz bazy danych MySQL) oraz usługę poczty, delegowaną do Gmail. Rozwiązanie to było proste i łatwe w zarządzaniu, jednak powodowało istotne problemy, zwłaszcza z bezpieczeństwem danych.



Największą wadą architektury, jaką dysponowaliśmy, była duża powierzchnia ataków - zainfekowany komputer webmastera infekował pliki stron www i rozprzestrzeniał się, także na urządzenia odwiedzających taką stronę. Wielokrotnie otrzymywaliśmy powiadomienia o istnieniu zainfekowanych plików i problemach ze starszymi stronami. Największym jednak problemem była niedbałość administratorów stron www, którzy nie wypełniali obowiązku aktualizowania stron. Między innymi można wymienić:

- stare strony pisane w PHP (często w PHP 5.2, gdy w sieci dostępny był PHP 5.6)
- strony zawierające fora internetowe na nieaktualizowanych silnikach - był jeden przypadek, gdy baza danych jednego z kont zajmowała ponad 500MB w 2014r.
- (głównie spam od botów), a silnik strony przestał być rozwijany w 2012r.
- największą plagą były jednak systemy CMS typu Joomla i Wordpress - wielokrotnie odnotowywaliśmy istnienie na serwerze wersji WP od 2.6 do 3.8, gdy tymczasem najnowszą dostępną wersją była 4.3-4.4 (Webmasterzy jednostek harcerskich nie aktualizowali systemów CMS przez 3 i więcej lat!)

Nie mogliśmy przeciwdziałać temu w prosty sposób, gdyż:

- Naczelnictwu zależało na zachowaniu w postaci niezmienionej rysu historycznego ZHR, w postaci starych stron www
- Nie posiadaliśmy aktualnych informacji o osobach odpowiedzialnych za strony www

- W przypadku blokady kont, które rażąco naruszały bezpieczeństwo - osoby z kręgu zarządzającego jednostką, której strona została zablokowana straszyli skargami do Naczelnictwa.
- Nie mieliśmy statutowych/legalnych możliwości przymuszenia użytkowników do dbania o aktualność stron www.

Z braku instrumentów jakimi moglibyśmy przeciwdziałać zaniedbaniom ze strony użytkowników serwera, skazani byliśmy na weryfikację i powolną modernizację serwera.

Przewidywano następujące etapy działań:

1. weryfikacja danych osób odpowiedzialnych za strony www jednostek
2. wykonanie aktualizacji stron jednostek istniejących
3. Konwersja stron archiwalnych - nieistniejących już drużyn - ze stron dynamicznych (PHP) do stron statycznych (HTML).

Równolegle do tych działań miała odbywać się modernizacja samego serwera i sposobu udostępniania treści użytkowników. Niestety, przy niewystarczających nakładach sprzętowych nie można było przeprowadzić tej modernizacji w szybki sposób. Głównym problemem były braki sprzętowe i kadrowe. Część z osób, które tworzyły Matrix odeszła na inne pola służby. Brakowało też chętnych, którzy chcieliby pomagać przy pracach.

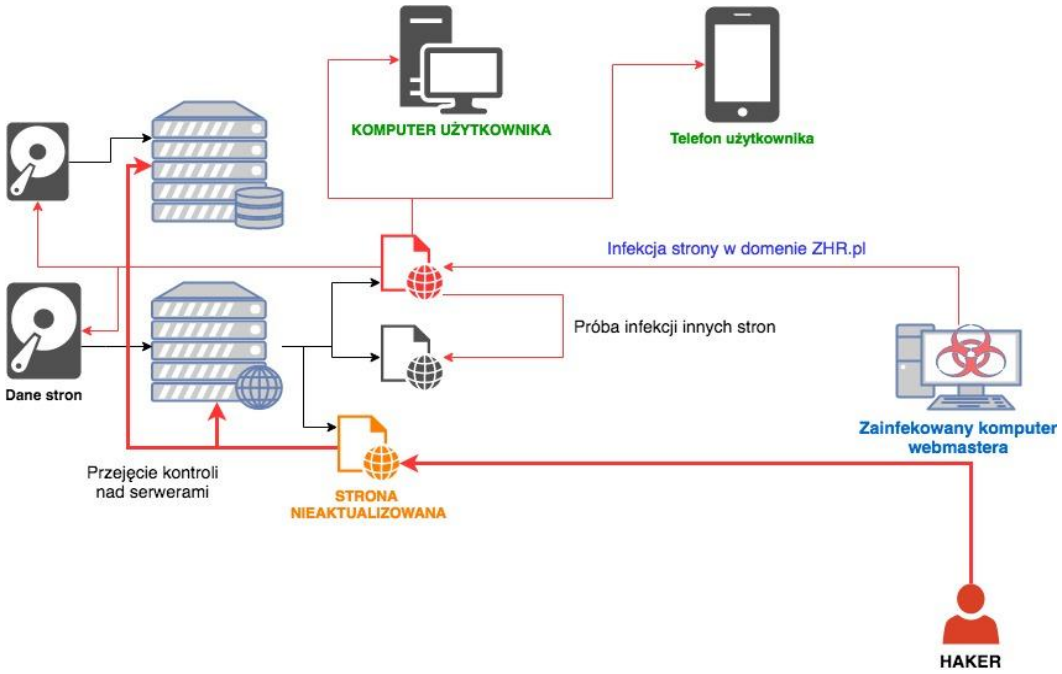
Brak informacji kontaktowych do osób odpowiedzialnych za strony www, utrudniał ich aktualizację. W końcowym efekcie niezaktualizowane strony www przyczyniły się do ataków na serwer.

W związku z licznymi atakami na ZHR.pl zablokowano dostęp z całych bloków adresowych, m.in. z krajów takich jak Chiny, Indie, Tajlandia, Argentyna. Działanie to ograniczyło ilość ataków.

Zabezpieczanie usług, przy nieaktualizowanych stronach www jednostek, pochłonęło ogromne ilości pracy i wstrzymało weryfikację kont, czy też samą modernizację istniejącej infrastruktury. Ostatecznie poskutkowało to poważnym atakiem - który miał miejsce ponad rok temu.

W wyniku wykorzystania jednej z podatnych stron, zaatakowano sam serwer i przejęto nad nim kontrolę - atakujący zmienił hasła dostępu do serwera i zablokował dostęp administratorom. Przywracanie dostępu do danych administracyjnych na serwerze było czasochłonne. Jednak nie można było samego serwera wystawić znów do sieci, dopóki nie namierzono źródła ataku. Stąd niedostępność usług przez długi czas. Zaistniałą sytuację wykorzystaliśmy do przeprojektowania działania samego serwera, lepszej izolacji stron www, co utrudniłoby ponowny atak.

Innym poważnym problemem poprzedniego rozwiązania była nieunormowana sytuacja z serwerownią. Do tej pory nasze maszyny trzymane były w serwerowni firmy INEA za darmo i bez żadnej umowy. Skutkiem takiej sytuacji było ograniczenie przepustowości łącza naszego serwera do minimum (ok. 250 kbps) z winy dużej ilości spamu rozsyłanego przez niezabezpieczone strony jednostek.



2. Obecna architektura

a. Całkowite wyłączenie serwera pozwoliło nam na kompletne przeprojektowanie architektury. Postawiliśmy na chmurę docker swarm. Pozwoliło nam na to uzyskanie drugiego serwera od Macieja Konusa Kamińskiego.

b. Unormowana została też sytuacja z serwerownią. Mamy obecnie podpisaną umowę z firmą Skynet gdzie odpłatnie (za niewielkie pieniądze) trzymamy dwa serwery oraz switch.

c. Rozwiązanie chmurowe, które zastosowaliśmy zabezpiecza nas przed awarią jednej z fizycznych maszyn. W razie wystąpienia takiej sytuacji ruch kierowany jest na zdrową maszynę. Dodatkowo pozwala to na łatwe skalowanie w przypadku zakupienia następnego serwera.

d. Zmianie uległo bezpieczeństwo samego serwera - pojedyncza strona nie zagraża już teraz innym treściom, czy samemu serwerowi. Osiągnięto to, dzięki:

- zamknięciu stron w odosobnionych kontenerach
- dla systemów CMS utworzono domyślne obrazy - użytkownik nie musi pamiętać o aktualizacji Wordpressa, gdyż wystarczy uaktualnienie obrazu przez administratora i wszystkie strony otrzymają zaktualizowany system treści
- użycie kontenerów zapewnia izolację od maszyny i sprzętu - atakujący może przejąć tylko sam kontener, ale będzie mu bardzo trudno uzyskać coś więcej i nie będzie w stanie odciąć administratorów od maszyny.
- zyskano przenośne rozwiązanie - łatwiej jest zmigrować kontener danej strony na inną maszynę o podobnej konfiguracji do serwera - wystarczy przenieść obraz i dane konta www, by strona działała w sposób prawie niezauważalny dla użytkownika
- jeśli dojdzie do zainfekowania plików strony w kontenerze, dla których istnieje obraz startowy, to wystarczy restart kontenera, by pozbyć się "niechcianych dodatków" do strony. Przywrócone zostaną pliki odpowiedzialne za wygląd i zachowanie strony zgodnie z obrazem startowym - wszystkie zmiany w zachowaniu strony, np. skrypty, które na komputerach oglądających stronę próbują instalować złośliwe oprogramowanie, znikną po restarcie kontenera.
- system kontenerów pozwala na efektywne zarządzanie kontami użytkowników.

Jedyną wadą jest nakład kosztów (zwłaszcza pracy) dla przygotowania takiego środowiska i odpowiadającej mu dokumentacji. Są to prace czasochłonne, jednak niezbędne dla prawidłowego utrzymania serwera i dalszego rozwoju usług w domenie ZHR.pl

Dodatkowo cała architektura ma być docelowo wspierana przez narzędzia jak:

- JIRA
- Confluence
- JIRA ServiceDesk

Które są powszechnie znane jako narzędzia organizacji pracy, dokumentacji oraz zarządzania incydentami. Wdrożenie tych narzędzi (które trwa obecnie) zapewni wyższy standard pracy, a jednocześnie może być doskonałą sposobnością dla młodych adeptów informatyki, chcących zapoznać się z komercyjnymi narzędziami i metodykami pracy w organizacji.

Istotną kwestią jest przyszłość Matrixa i jego dalszy rozwój. Osoby pracujące nad utrzymaniem dostępności i ciągłości usług ZHR.pl powinny mieć zapewnione narzędzia poza techniczne, tj. możliwość podejmowania działań w sposób autonomiczny w ramach ich kompetencji. Przykładem może być blokowanie kont (www, pocztowych), które rażąco naruszają bezpieczeństwo lub są niezgodne z obowiązującym prawodawstwem. Przy tego typu działaniach powinny zostać wypracowane procedury postępowania - np. jeśli poczta w domenie ZHR.pl jest wykorzystywana do rozsyłania spamu, to konto spamujące jest blokowane, sporządzana jest notatka/zgłoszenie do zwierzchnika harcerza, jednostki, okręgu, akcji, czy też informowane jest samo Naczelnictwo. Jest to szczególnie istotne w kwestii zmiany przepisów dotyczących ochrony danych osobowych - słynne RODO. Wszystkie procedury powinny być spójne, jednoznaczne i dostępne dla Mx i Naczelnictwa.

Przed włączeniem całej usługi chmurowej dla wszystkich jednostek wstrzymuje nas jeszcze kilka spraw:

- stworzenie porządnej dokumentacji naszych narzędzi - to zdecydowanie usprawni nasze działania i przyspieszy reakcję na problemy oraz rozwój usług.
- przeprojektowanie regulaminu kont pod względem nowej architektury i przepisów (m.in. RODO)
- Skonfigurowanie panelu do zgłaszania problemów dla użytkowników, który automatycznie będzie przydzielał zadania (taski) do członków Matrixa
- Aplikacja do rejestracji nowych użytkowników, która jako potwierdzenie tożsamości będzie wykorzystywała okręgi, a nie członków Matrixa. Nasz zespół nie zna wszystkich instruktorów, więc do tej pory nie mieliśmy możliwości weryfikacji kto zakłada dane konto i czy nazwa jest adekwatna do jednostki. Nowa koncepcja takiej aplikacji zakłada przy rejestracji użytkownika wskazanie okręgu, z którego jest jednostka. Aplikacja prześle e-mail z linkiem weryfikacyjnym do okręgu i dalej dany okręg będzie mógł zweryfikować poprawność danych. Dodatkowo usprawni to pewną odpowiedzialność za konta. Do tej pory w żaden sposób nie mogliśmy wyegzekwować od użytkowników trzymania się zasad zawartych w naszym regulaminie. Liczymy tutaj na mocne wsparcie ze strony okręgów.

Zespół wykonał ogromną część pracy, którą nie bardzo jeszcze widać na zewnątrz. Postawiliśmy wszystkie usługi zupełnie od nowa z uwzględnieniem nowoczesnych technologii. Jednak aby nasze usługi dalej się rozwijały potrzebujemy nowego, porządnego sprzętu. Podsiadamy dwa serwery, z których jeden był nową maszyną, którą staraniem Matrixa dostaliśmy za darmo od HP. Jednak urządzenie to ma już 8 lat. Drugi serwer także dostaliśmy za darmo, ale firma, która nam

go podarowała chciała go zutylizować. Nie możemy bazować na takim sprzęcie. Szczególnie, że nowa architektura zapewnia łatwe skalowanie. Potrzebujemy nowego serwera z prawdziwego zdarzenia. Wtedy starczyłoby też nam przestrzeni do tworzenia backupów.

Inną sprawą jest rozszerzenie zespołu. Ciężko jest zachęcić do pracy ludzi nie dając nic w zamian. To są ciężkie godziny wieczorne pracy, czasami nocne. Często musimy wyrwać się z pracy, żeby coś zrobić. Moim planem na zachęcenie do udziału w Matrixie są kursy i szkolenia dla członków Matrixa. Jednak aby takie szkolenia były atrakcyjne i coś dawały (np. certyfikaty przydatne w dalszej pracy zawodowej) także potrzebujemy wsparcia finansowego i organizacyjnego. Mamy szansę stworzyć miejsce, w którym ludzie mogliby doskonalić swoje umiejętności zawodowe.

3.Sytuacja dotycząca ZiHeRa:

Do tej pory większość okręgów używało programu napisanego 10 lat temu (tzw. stary ZiHeR). W związku ze zmianą przepisów (tzw. RODO) stary ZiHeR zostaje wyłączony pod koniec kwietnia tego roku gdyż nie spełnia on wymogów bezpieczeństwa oraz aktualnie nie da się go rozwijać. Od dawna trwały prace nad przepisaniem aplikacji w celu umożliwienia dodawania nowych funkcjonalności - od zeszłego roku pierwsze okręgi używają “nowego ZiHeRa”. Aktualnie nowej wersji używa 8 okręgów - wszystkie pozostałe mogą się przyłączyć. Nowy ZiHeR jest programem Open Source, z kodem źródłowym dostępnym w Internecie. W związku z czym każdy okręg, który chciałby dodać nowe funkcjonalności może to zrobić na własną rękę bądź we współpracy z Matrixem - najlepiej skontaktować się pod adresem ziher@zhr.pl