Czytaj lub słuchaj artykuł online

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

https://xo.pl/it-na-wesolo-sec-firewall

BEZPIECZEŃSTWO IT

Firewall, czyli przejście graniczne Republiki Pakietów

W Republice Pakietów każdy mieszkaniec miał adres, każda usługa swoje drzwi, a na granicy stał szlaban. Przez lata działało to całkiem nieźle, dopóki Pan Kierownik nie został Ministrem Usprawniania Ruchu. Pierwszego dnia przyjechał służbową limuzyną, zobaczył kolejkę ciężarówek i ogłosił reformę, która niemal zakończyła istnienie republiki przed drugim śniadaniem. 🛂🚧🤣

— PANIE GRZESIU! — zawołał do komendanta straży granicznej. — DLACZEGO TU STOJĄ SAMOCHODY?!

— Bo sprawdzamy, dokąd jadą i czy wolno im przejechać.

— ALE ONE CHCĄ JECHAĆ!

— Właśnie dlatego mamy szlaban. Gdyby nie chciały, kontrola byłaby zbędna.

Pani Agnieszka, szefowa ewidencji granicznej, spojrzała na plik ministerialnych rozporządzeń.

— Panie Ministrze, proszę najpierw zapoznać się z zasadami.

— ZASADA NUMER JEDEN: ŻADNYCH KOLEJEK!

Grzesiu zamknął oczy. Republika Pakietów dopiero się budziła. Kłopoty już były na nogach.

Granica, która nie rozpoznaje dobrych intencji

Grzesiu pokazał ministrowi mapę. Po jednej stronie znajdowała się sieć urzędów, serwerów i mieszkańców republiki. Po drugiej — ogromny świat pełen zwyczajnych podróżnych, klientów, kurierów, a czasem także nieproszonych gości.

— Firewall, czyli zapora sieciowa, działa jak kontrola na granicy. Ocenia ruch według zdefiniowanych zasad i może go dopuścić, zablokować lub odrzucić. W rzeczywistości sprawdza między innymi adresy IP, protokoły, porty, kierunek ruchu i — jeśli potrafi — stan połączenia.

— CZYLI SPRAWDZA, CZY KTOŚ JEST UCZCIWY?

— Nie. Zwykła zapora nie czyta w myślach, nie rozpoznaje automatycznie każdego wirusa i nie zgaduje, czy człowiek ma złe zamiary.

— Ale jest na granicy! — oburzył się Minister.

— Celnik też może sprawdzić dokumenty ciężarówki. Nie wie od tego, czy kierowca jutro oszuka własną babcię.

Agnieszka dopisała do protokołu: „Zapora nie jest jasnowidzem”.

— TEGO NIE WPISUJEMY DO REKLAMY KRAJU! — zaprotestował Kierownik.

Wielkie Otwarcie Wszystkiego

Minister wdrapał się na skrzynkę po pomarańczach i wydał pierwsze zarządzenie.

— OTWORZYĆ WSZYSTKIE SZLABANY! NIECH GOSPODARKA ODDYCHA!

Grzesiu poprosił o rozkaz na piśmie. Agnieszka poprosiła o podpis. Minister podpisał trzy egzemplarze, z których jeden omyłkowo zatytułował „Menu obiadowe”.

Szlabany poszły w górę. Do Republiki wjechały dostawy, klienci i wycieczka szkolna. Zaraz za nimi pojawiła się ciężarówka z napisem „BEZPŁATNA KONTROLA WSZYSTKICH DRZWI”. Kierowca zatrzymywał się przy każdym budynku i próbował każdej klamki.

— CO ON ROBI? — zapytał Minister.

— Sprawdza, które usługi odpowiadają. Taki ruch może przypominać skanowanie portów. Samo skanowanie nie jest równoznaczne z udanym włamaniem, ale nie ma powodu wystawiać każdej wewnętrznej usługi całemu światu.

Za ciężarówką jechał bus, którego kierowca żądał wejścia do bazy księgowej.

— A ma uprawnienia? — zapytała Agnieszka.

— Nie pytał nikt, skoro szlaban otwarty — odparł kierowca.

— PANIE KIEROWNIKU, WŁAŚNIE PO TO ISTNIEJĄ REGUŁY! — zawołał Grzesiu.

— TO ZAMKNIEMY WSZYSTKO! — odpowiedział Minister. — I BĘDZIE BEZPIECZNIE!

Agnieszka nie zdążyła nawet przewrócić oczami.

Wielkie Zamknięcie Wszystkiego

O godzinie 9:17 wszystkie szlabany opadły. Zatrzymano dostawę leków do szpitala, paczki dla urzędu, klienta odwiedzającego publiczną witrynę i odpowiedź na zapytanie wysłane pięć sekund wcześniej.

— DOSKONALE! — oznajmił Minister. — NIKT NIEPOWOŁANY NIE PRZEJDZIE!

— Nikt powołany też — zauważyła Agnieszka.

— SZCZEGÓŁ!

Na granicy utknął kurier pocztowy.

— Mam wiadomości dla republiki!

— WSTĘP WZBRONIONY! — wrzasnął ministerialny megafon.

— Ale sami zamówiliśmy tę pocztę! — odkrzyknęła Agnieszka.

— Trudno. Bezpieczeństwo przede wszystkim!

Grzesiu poprowadził Ministra na wzgórze. W dole stały nieruchome auta, a za nimi cała gospodarka.

— Zapora, która blokuje każdą potrzebną usługę, nie chroni prawidłowo działającego systemu. Paraliżuje go. Ochrona ma umożliwiać bezpieczne korzystanie z sieci, a nie zamieniać ją w muzeum nieczynnych połączeń.

— ALE PRZYZNA PAN, ŻE NIKT NAS TERAZ NIE ATAKUJE!

— Nie ma też komu wystawić faktury za pańską pensję.

— AGNIESZKO! PILNIE OTWORZYĆ KSIĘGOWOŚĆ!

Regulamin zamiast nastroju ministra

Agnieszka wyciągnęła czystą kartkę i zaczęła spisywać zasady. Każda reguła określała, jaki ruch ma przejść, a jaki nie. Grzesiu narysował trzy kolumny: skąd, dokąd i po co.

— Na przykład mieszkańcom pozwalamy wychodzić do potrzebnych usług, publiczny serwer WWW wystawiamy dla odwiedzających, a wewnętrzna baza danych nie musi być dostępna z Internetu — powiedział.

— A jeśli ktoś zapyta, jaką ma przepustkę? — zainteresował się Minister.

— W praktyce zapora może sprawdzać źródłowy i docelowy adres IP, protokół, port źródłowy i docelowy, interfejs oraz stan połączenia. Konkretne możliwości zależą od urządzenia i jego konfiguracji.

— Czyli IP to nazwisko?

— W tej analogii raczej adres początkowy i docelowy. Port to nie numer domu, tylko wskazanie konkretnej usługi w urządzeniu. I uwaga: numer portu nie gwarantuje, jaki program rzeczywiście tam działa.

Agnieszka postawiła pieczątkę pod zasadą: „Najpierw przepuszczamy to, co uzasadnione. Resztę oceniamy według polityki”.

— Możemy stosować domyślne blokowanie tam, gdzie dokładnie znamy wymagane usługi. Na granicy sieci firmowej często to rozsądny punkt wyjścia. Ale nie jest to polecenie, by bez analizy zamknąć każdy port każdemu pracownikowi.

— A MOJA POPRZEDNIA ZASADA „WSZYSTKO WOLNO”?

— Właśnie ją zastępujemy procedurą.

— OKRUTNA TA ADMINISTRACJA!

Kolejność pieczątek ma znaczenie

Minister postanowił ułatwić Agnieszce pracę. Na pierwszej stronie regulaminu dopisał wielkimi literami „WPUSZCZAĆ WSZYSTKICH”, a pod spodem kilkanaście zakazów.

— No i jest kompletna lista! — ucieszył się.

— Nie w systemie, w którym reguły sprawdza się po kolei i pierwsza pasująca kończy ocenę — wyjaśnił Grzesiu. — W takim przypadku późniejsze zakazy mogą nigdy nie zadziałać.

— To co, kolejność jest ważna?

— W wielu zaporach tak. Nie we wszystkich mechanizm jest identyczny, dlatego trzeba znać zachowanie konkretnej platformy. Reguły zbyt ogólne mogą przysłaniać te szczegółowe.

Agnieszka przekreśliła ministerialny dopisek.

— Może pan napisać swoje życzenie w osobnym zeszycie.

— A KTO GO PRZECZYTA?

— Na razie nikt nie zgłosił takiej potrzeby.

Pan z odpowiedzią, którego nikt nie rozpoznaje

Do szlabanu podjechał niewielki samochód. Za kierownicą siedział kurier z pieczątką „ODPOWIEDŹ”.

— Jadę do pani Agnieszki! To ona wysłała zapytanie!

— Proszę pokazać przepustkę! — krzyknął młody strażnik.

— Nie mam. Ale mam numer sprawy!

Grzesiu otworzył rejestr połączeń.

— Tutaj wchodzi stateful firewall i conntrack, czyli śledzenie stanu przepływów. Gdy urządzenie widzi dozwolone połączenie wychodzące, może rozpoznać pasujący ruch powrotny i przepuścić go bez tworzenia osobnej, szerokiej reguły wpuszczającej świat do środka.

— A gdybyśmy nie mieli rejestru? — zapytała Agnieszka.

— Zapora stateless ocenia pakiety bez takiego kontekstu połączenia. Trzeba wtedy opisać dozwolony ruch odpowiednio w obu kierunkach. W praktyce różne protokoły wymagają różnego sposobu śledzenia — to nie zawsze jedna prosta „rozmowa”.

Minister spojrzał w rejestr.

— TO ZNACZY, ŻE JAK KTOŚ WYJECHAŁ, TO KAŻDY MOŻE ZA NIM WRÓCIĆ?

— Nie. Odpowiedź musi pasować do śledzonego przepływu i polityki zapory. Sam napis „ODPOWIEDŹ” na masce auta niczego nie załatwia.

— SZKODA. JUŻ ZAMÓWIŁEM PIECZĄTKI.

Trzy drogi: do strażnicy, przez republikę i ze strażnicy

Agnieszka rozłożyła przed ministrem mapę z trzema kolorowymi strzałkami.

— Jeżeli pakiet jest skierowany do samego urządzenia z firewallem, to inna sytuacja niż pakiet, który tylko przez to urządzenie przejeżdża. A jeszcze inna, gdy ruch tworzy sam router.

— I to ma znaczenie?

— Ogromne. W znanym administratorom modelu Linuxa mamy łańcuchy takie jak INPUT, FORWARD i OUTPUT. INPUT dotyczy lokalnego celu, FORWARD przekazywania dalej, OUTPUT ruchu generowanego lokalnie. Dokładny sposób obsługi zależy od stosu i konfiguracji.

— Czyli jeśli zamknę wejście do strażnicy, to niekoniecznie zamknę autostradę przez republikę?

— Właśnie. Nie mieszamy ochrony samego routera z filtrowaniem pakietów tranzytowych.

Minister zamyślił się.

— A jeśli zamknę wszystkie trzy?

— To znowu będziemy mieli godzinę 9:17 — odpowiedziała Agnieszka.

Biuro Zmiany Adresów nie jest policją graniczną

Obok przejścia działało Biuro Numeracji. Każdy samochód wyjeżdżający z prywatnej dzielnicy otrzymywał na zewnątrz wspólny adres republiki, a biuro zapisywało, komu przypisało odpowiednią odpowiedź.

— Genialne! — zawołał Minister. — NAZWĘ TO NAJLEPSZYM FIREWALLEM!

— Nie — zaprotestował Grzesiu. — To analogia do NAT, czyli translacji adresów. NAT zmienia informacje adresowe, a często także porty. Może współpracować ze śledzeniem połączeń i utrudniać niektóre niezamówione wejścia z zewnątrz, lecz sam NAT nie jest polityką bezpieczeństwa firewalla.

— Czyli zmiana tablic rejestracyjnych nie oznacza, że kierowca przeszedł kontrolę?

— Dokładnie. Można tłumaczyć adresy i filtrować ruch osobnymi mechanizmami, nawet jeśli router wykonuje obie rzeczy.

— Ale z nową tablicą wygląda bardziej oficjalnie! — bronił się Kierownik.

— To może pan też sobie kupić czapkę celnika. Nadal nie będzie pan firewallem.

Strefy zaufania, czyli nie każdy ma klucz do skarbca

Po południu do odprawy zgłosił się pojazd z napisem „GOŚCIE WI-FI”. Kierowca prosił o dojazd prosto do skarbca z dokumentami księgowymi.

— Przecież jest już na naszym terenie — zauważył Minister.

— I co z tego? — zdziwiła się Agnieszka. — Gość restauracji też nie dostaje klucza do sejfu.

— Sieć warto dzielić na strefy — wyjaśnił Grzesiu. — Publiczne serwery, urządzenia administracyjne, sieć pracowników i goście Wi-Fi nie muszą mieć tych samych uprawnień. Zapora może kontrolować ruch między strefami, nie tylko na granicy z Internetem.

— Czyli nawet wewnętrzny ruch czasem trzeba ograniczyć?

— Tak. Przejęcie jednego komputera nie powinno automatycznie otwierać dostępu do wszystkich systemów w firmie.

— TO KAŻDY PRACOWNIK DOSTANIE WŁASNE PAŃSTWO! — zarządził Minister.

— Zacznijmy od sensownych sieci VLAN i reguł między nimi — odparł Grzesiu. — Mapy nie muszą być aż tak ambitne.

Dziennik graniczny, czyli „dlaczego to nie działa?”

O 14:26 ktoś zadzwonił z urzędu.

— Nie działa nam drukarka sieciowa!

Minister rozpromienił się.

— MOŻE TO ATAK! ZAMKNĄĆ GRANICĘ!

— Najpierw sprawdźmy logi — powiedział Grzesiu.

Agnieszka otworzyła dziennik: data, godzina, źródło, cel, protokół, port i decyzja. Widać było, że nowa reguła odcinała ruch potrzebny drukarce.

— Czyli problemem nie jest haker, tylko nasz regulamin?

— Tym razem tak. Logowanie, liczniki reguł, testy oraz świadome wyjątki pomagają diagnozować problemy. Nie należy jednak bezmyślnie zapisywać każdego pakietu bez ograniczeń, bo można zalać dyski i zgubić ważne zdarzenia w hałasie.

— TO JA ZALOGUJĘ WSZYSTKO, ŁĄCZNIE Z GOŁĘBIAMI! — oznajmił Minister.

— Właśnie przed chwilą powiedziałem, żeby tego nie robić.

— A JAK INACZEJ BĘDZIEMY WIEDZIELI, KTO LATA?!

Przywrócili potrzebny ruch. Drukarka wypluła trzydzieści siedem stron testowych. Minister kazał wszystkie zachować jako dowód skuteczności reformy.

Celnik od bagażu to nie wróżbita

Na granicy pojawił się nowy mundurowy. Potrafił nie tylko czytać tablice rejestracyjne, lecz także zaglądać głębiej do niektórych ładunków.

— To jest lepszy firewall? — zapytała Agnieszka.

— Niektóre zapory mają filtrowanie aplikacyjne, inspekcję ruchu, IDS lub IPS. Mogą analizować więcej niż same adresy i porty oraz rozpoznawać pewne wzorce ataków. Ale zakres widoczności zależy od protokołów, szyfrowania, ustawień i możliwości urządzenia.

— Czyli skoro mamy takiego celnika, to nie potrzebujemy innych zabezpieczeń?

— Potrzebujemy. IDS przede wszystkim wykrywa i alarmuje, IPS może blokować według swoich reguł. Żaden system nie gwarantuje wykrycia wszystkich zagrożeń. Aktualizacje, kontrola dostępu, kopie zapasowe i rozsądne działania ludzi nadal mają znaczenie.

— A MOŻE ZATRUDNIMY WRÓŻKĘ? — zainteresował się Minister.

— Jeśli będzie umiała odczytać logi, rozważę kandydaturę — odparł Grzesiu.

Najbardziej niebezpieczna przepustka

Tuż przed zamknięciem zmiany przez granicę przeszedł legalnie mieszkaniec republiki. Miał prawidłowe dokumenty, dozwolony kierunek i zgodę na kontakt z zewnętrznym serwisem. W środku spotkał człowieka, który przekonał go, że dla bezpieczeństwa powinien natychmiast podać hasło i zatwierdzić obce logowanie.

— PRZECIEŻ PRZESZEDŁ PRZEZ NASZĄ KONTROLĘ! — oburzył się Minister.

— Tak. Bo jego połączenie było dozwolone. Zapora nie mogła wiedzieć, że użytkownik właśnie da się nabrać na **phishing** — odpowiedział Grzesiu.

— To po co nam cały ten szlaban?

— Żeby ograniczać określone rodzaje niepożądanego ruchu i utrudniać ataki. Ale firewall nie zastępuje człowieka, aktualizacji systemów ani **silnych haseł i MFA**. Nawet dozwolony ruch może nieść zagrożenie, a legalny użytkownik może popełnić błąd.

Agnieszka odłożyła raport.

— Czyli nie mamy magicznej granicy, która ochroni republikę przed każdym głupim pomysłem?

— Gdyby istniała — westchnął Grzesiu — zaczęlibyśmy od gabinetu Ministra.

— SŁYSZAŁEM! — dobiegło zza drzwi.

— Taki był zamiar.

Rozsądna granica, żywa republika

Następnego ranka kolejki zniknęły. Nie dlatego, że otwarto wszystko, lecz dlatego, że ustalono sensowne reguły, sprawdzono potrzebne usługi i usunięto przypadkowe blokady. Kurierzy przejeżdżali, mieszkańcy korzystali z sieci, a nieproszony ruch nadal zatrzymywał się przed szlabanem.

Minister zwołał konferencję.

— OGŁASZAM, ŻE NASZA GRANICA JEST IDEALNA! NIC ZŁEGO JUŻ NIGDY SIĘ NIE WYDARZY!

— Nie — powiedzieli jednocześnie Agnieszka i Grzesiu.

— TO CO MAM OGŁOSIĆ?!

— Że firewall działa zgodnie z potrzebami republiki, reguły są udokumentowane i testowane, a incydenty analizujemy. I że nie da się zastąpić rozsądku jednym urządzeniem.

— A MOŻE PRZYNAJMNIEJ ZAMKNIEMY CAŁKIEM GRANICĘ NA WEEKEND?

— Nie. Szpital potrzebuje dostaw, a obywatele Internetu.

— TO OTWÓRZMY WSZYSTKIE BRAMKI TYLKO W PIĄTEK!

Agnieszka wręczyła mu dokument.

— Co to? — zapytał.

— Regulamin. Jedyny papier, którego pan dziś nie może przerobić na samolocik.

Dobry firewall nie wpuszcza każdego, ale też nie zatrzymuje całego życia. Przepuszcza uzasadniony ruch według przemyślanych reguł, pozwala diagnozować błędy i stanowi jedną z warstw ochrony. Zbyt łagodny pozostawia zbędnie otwarte drzwi. Zbyt restrykcyjny potrafi zepsuć działanie usług. A przed bezmyślnością użytkownika żaden szlaban nie daje stuprocentowej gwarancji.

Ministerstwo Usprawniania Ruchu Republiki Pakietów informuje: szlabany działają, kurierzy wrócili na trasy, rejestr połączeń odzyskał sens, a pani Agnieszka odnalazła faktury za trzy nieudane reformy graniczne. Panu Kierownikowi odebrano prawo do wydawania zarządzeń przez megafon. W odwecie próbował odblokować port 65536. Straż graniczna poinformowała go, że takiego portu nie ma. 🛂🚧🤣❤️