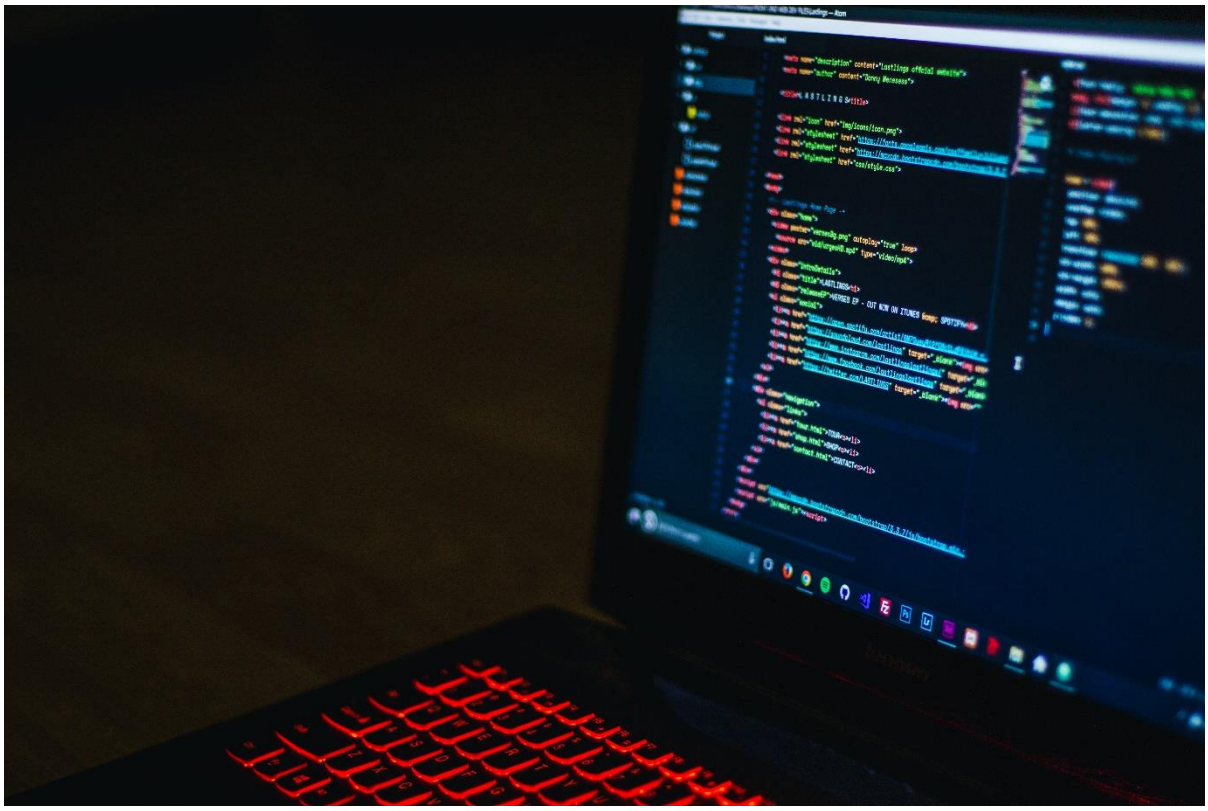
ZYXEL

Dobre, złe i brzydkie aspekty implementacji zabezpieczeń sieciowych

Jeśli miałaby istnieć nowoczesna wersja dawnego amerykańskiego dzikiego zachodu, byłby nią świat online. Internet i podłączone do niego urządzenia generują okazje, z których korzystają przestępcy, a egzekwowanie prawa jest… minimalne. Podobnie jak w słynnym westernie z Clintem Eastwoodem, często jedynym rozwiązaniem jest wzięcie sprawy w swoje ręce lub współpraca z ludźmi, którzy mogą ci pomóc ponieważ dysponują specjalistyczną wiedzą.



Sprawdź, w jaki sposób możesz ukierunkować swojego wewnętrznego Clinta, aby móc rozpoznawać zagrożenia i jak zatrzymać cyberprzestępców poza miastem (a przynajmniej poza siecią).

Złe

Cyberprzestępczość jest wszędzie wokół nas i przybiera na sile. Wszelkiego rodzaju dane, nawet te pozornie nieszkodliwe, można sprzedawać i kupować w sieci darknet. Mogą one zostać wykorzystane w przestępstwach wszelkiego rodzaju, od szantażu po kradzież tożsamości. Cyberprzestępczość jest obecnie wysoce dochodową, bardzo wyrafinowaną branżą, a jeśli masz sieć, jest bardzo prawdopodobne, że ktoś spróbuje ją złamać.

Według danych Światowego Forum Ekonomicznego obecne trendy cyberprzestępczości, obejmują ataki na zdalny dostęp, przeprowadzane za pomocą smartfona, luki w automatyce domowej i internecie rzeczy (IoT) oraz obchodzenie tradycyjnych zabezpieczeń przed cyberprzestępczością przy użyciu sztucznej inteligencji (AI).

Ochronie podlega nie tylko sieć, ale również ogromna liczba podłączonych do niej urządzeń. Nie wszystkie są „tradycyjnymi" urządzeniami, takimi jak komputery czy telefony. Co więcej, środki, na których wcześniej polegaliśmy, takie jak tradycyjne zapory sieciowe i programy antywirusowe, nie są już wystarczające, ponieważ cyberprzestępcy mogą je złamać - jeśli nie dzisiaj, to prawie na pewno w najbliższej przyszłości.

Brzydkie

Brzydka prawda wygląda tak, że menedżerowie sieci muszą myśleć jak cyberprzestępcy, aby móc ich pokonać. Muszą przewidywać ich ruchy, zrozumieć sposób myślenia i monitorować zachowanie.

Urząd do spraw statystyki krajowej w Wielkiej Brytanii oświadczył, że ludzie są bardziej narażeni na cyberprzestępczość niż na jakikolwiek inny rodzaj przestępstwa. Przestępcy w tym obszarze są bardzo sprytnymi operatorami, a ich własne sieci są bardzo rozbudowane i responsywne. Małe firmy stanowią ogromną większość przedsiębiorstw w Wielkiej Brytanii, dlatego tamtejsi hakerzy są niezwykle „zapracowani": małe firmy z Wielkiej Brytanii w sezonie 2017/2018 zmagały się średnio z pięcioma cyberatakami rocznie.

Dobre

Dobra wiadomość jest taka, że firmy, użytkownicy indywidualni, jak i gospodarstwa domowe, mogą teraz zaimplementować niedrogą i inteligentną ochronę przed cyberprzestępczością. W przypadku firm można ją skonfigurować tak, aby obejmowała całą sieć i podłączone do niej urządzenia. Biorąc jednak pod uwagę złożoność i skalę omawianych problemów, wiele osób jest zaskoczonych dostępnymi opcjami i nie ma pewności, czego dokładnie potrzebują.

Cyberprzestępczość jest szybko ewoluującym sektorem, który wykorzystuje sztuczną inteligencję i uczenie maszynowe, przez co codzienne ataki są coraz bardziej wyrafinowane. Właśnie dlatego potrzebne jest oprogramowanie zabezpieczające, które może zrobić to samo i zwalczyć ogień ogniem.

Wraz z dynamicznym rozwojem Internetu Rzeczy, komputery nie są jedynymi urządzeniami, które trzeba chronić. Większość z nas posiada smartfon, który działa online, coraz częściej instalujemy inteligentne systemy ogrzewania, oświetlenia i bezpieczeństwa. Są one podatne na ataki i również muszą być chronione.

Oto podstawowa lista atrybutów, których należy szukać w usługach zabezpieczających sieci:

- **Anty-wirus** – musi nieustannie skanować pliki pod kątem najnowszych zagrożeń, powinien zapewniać prawdziwą ochronę w czasie rzeczywistym i nie może polegać na ręcznych aktualizacjach wykonywanych przez użytkownika. System taki powinien wykraczać poza ochronę antywirusową, obejmując wszystkie złośliwe oprogramowania w tym trojany, oprogramowanie ransomware, robaki, oprogramowanie złośliwe i szpiegujące. Rozmiar pliku powinien być nieograniczony, a ochrona powinna być w stanie działać przy optymalnych ustawieniach bez obniżania wydajności sieci.
- **Sandboxing** – umożliwia izolację plików w bezpiecznym środowisku oraz konfigurację zabezpieczeń, które umożliwiają wysyłanie podejrzanych plików do chmury i sprawdzanie ich pod kątem złośliwego

oprogramowania. W przeciwieństwie do tradycyjnych usług, ochrona sieci, która obsługuje ten tryb, wychwytuje potencjalnie szkodliwe pliki, zanim będą w stanie spowodować jakiekolwiek szkody.

- **Anty-SPAM** – powinien działać za pośrednictwem protokołów SMTP i POP3, oferować ochronę przed wirusami w czasie rzeczywistym, posiadać filtr reputacji adresów IP oparty na nadawcy oraz obsługę czarnej i białej listy.
- **Ochrona aplikacji** – ta funkcja powinna umożliwiać szczegółową kontrolę nad ważnymi aplikacjami oraz identyfikacje i kontrolę ich zachowania, w tym przepustowości. Powinna wspierać niezawodne uwierzytelnianie użytkowników oraz generować statystyki i raporty w czasie rzeczywistym.
- **Filtrowanie treści** – powinno korzystać z dynamicznej bazy danych w chmurze, aby zapewnić zawsze aktualną ochronę. Duże korzyści oferują również funkcje SafeSearch oraz GeoIP do śledzenia adresów IP.
- **Wykrywanie i zapobieganie włamaniom** – w przypadku podejrzanych lub złośliwych działań system ochrony przed cyberprzestępczością powinien je wykrywać i ostrzegać o nich w czasie rzeczywistym. Profil zabezpieczeń powinien być konfigurowalny.

Cyberprzestępcy są często większymi ekspertami w manipulowaniu sieciami i danymi niż ich właściciele. Prawdą jest również, że zasięg i złożoność cyberprzestępczości zagraża nam wszystkim. Posiadanie najwyższej klasy ochrony sieci jest dziś elementem obowiązkowym, jeśli jeszcze go nie masz, nie warto zwlekać z tym dłużej.

Thorsten Kurpjuhn, menedżer ds. rozwoju europejskiego rynku bezpieczeństwa w Zyxel

Zyxel Communications

Zyxel Communications już od prawie 30 lat łączy ludzi koncentrując się na wdrażaniu innowacyjnych rozwiązań dla swoich klientów. Nasze możliwości adaptacji oraz innowacyjne technologie sieciowe czynią nas liderami komunikacji dla firm telekomunikacyjnych, dostawców usług, klientów biznesowych i użytkowników domowych.

- 1500+ współpracowników na całym świecie
- 100 milionów urządzeń łączących na globalną skalę
- Ponad 700,000 firm pracujących lepiej, dzięki produktom marki Zyxel
- Obecność na 150 światowych rynkach

Obecnie, Zyxel Communications tworząc sieci przyszłości, uwalnia potencjał i spełnia wymagania nowoczesnych miejsc pracy – wspierając ludzi w biurze, codziennym życiu i w czasie wolnym.

ZYXEL – twój sieciowy sojusznik

Dołącz do nas na Facebooku i LinkedIn!