Co to jest firewall?

1. Co to jest i do czego służy system firewall?

System firewall jest kluczowym elementem cyberbezpieczeństwa w każdej organizacji korzystającej z sieci Internet. Na infrastrukturę bezpieczeństwa IT składa sie wiele elementów, jednak gdybyśmy musieli wymienić tylko jeden, najbardziej krytyczny, to z całą pewnością byłby to firewall. Firewall jest bramą pomiędzy "światem zewnętrznym" – siecią Internet, a wewnętrzną infrastrukturą naszej organizacji. Jego kluczowym zadaniem jest zatrzymanie i odseparowanie zewnętrznych zagrożeń, tak aby nasza sieć mogła funkcjonować bez przeszkód. Zagrożenia zewnętrzne są stosunkowo dobrze znane także laikom nieinteresującym się na co dzień bezpieczeństem IT. Słyszymy o nich, a właściwie o ich skutkach, w codziennych wiadomościach: wirusy, robaki, konie trojańskie, ransomware, ukierunkowane ataki hakerskie – ich ofiarą padają największe firmy oraz organizacje rządowe, a skala zniszczeń, zarówno w sensie finansowym, jak i społecznym (utracona reputacja) bywa kolosalna. Terminem "**mallware**" (złe oprogramowanie) określamy całokształt wyżej wymienionych zagrożeń. W jaki sposób może on przeniknąć do naszej sieci komputerowej? Dróg ataku jest wiele – może on być zainicjowany poprzez: załącznik poczty elektronicznej, skrypt ukryty na odwiedzonej stronie WWW, zainfekowane narzędzie, np. darmowy program użytkowy lub sterownik pobrany z sieci. Możemy też paść ofiarą aktywnego ataku: haker może dostać się bezpośrednio do naszej sieci i umieścić zainfekowane pliki na serwerze, może też po prostu zdalnie przejąć kontrolę nad naszą infrastrukturą bez wprowadzania złośliwego oprogramowania. Często spotykaną opinią, zwłaszcza w odniesieniu do ataków hakerskich jest: "mnie to nie dotyczy", "jesteśmy za mali, aby ktoś się nami interesował". Niestety nie jest to prawdą. O ile rzeczywiście małe firmy nie są na celowniku wysoce wykwalifikowanych cyberprzestępców i nie staną się raczej ofiarami "ręcznie" przeprowadzonego wyrafinowanego ataku, to w Internecie funkcjonują tysiące zautomatyzowanych skryptów, które nieustannie przeczesują całą przestrzeń adresową sieci w poszukiwaniu dziur bezpieczeństwa. W razie znalezienia takowej, instalowany jest automatycznie mallware, a organizator takiego procederu dodaje przejęte zasoby do swojej kolekcji - tak powstaje tzw. "botnet", czyli zbiór zainfekowanych, podłączonych do sieci komputerów pozostających pod kontrolą hakera. Największe botnety liczą po kilka milionów komputerów osobistych, szacuje się, że w Polsce jest zainfekowanych w ten sposób co najmniej pół miliona komputerów. Innego rodzaju zagrożenie, bardzo niebezpieczne zwłaszcza dla małych firm, to różnego rodzaju ataki na systemy e-bankowości prowadzone za pośrednictwem mallware.

W przypadku opisanych wyżej scenariuszy lekarstwem na zagrożenie jest właśnie system firewall – dużo łatwiej filtrować i monitorować ruch sieciowy centralnie, tj. na styku z Internetem niż na poziomie każdego komputera PC i każdego serwera. W praktyce zabezpieczenie każdego komputera przed atakiem sieciowym jest po prostu niemożliwe do zrealizowania, choćby dlatego, że łatki bezpieczeństwa są udostępniane przez producentów z pewnym opóźnieniem, tak więc zawsze istnieje okno czasowe, w którym nasze komputery podatne są na atak.

Zasadę działania systemów firewall najprościej wyjaśnić przyglądając się ich ewolucji. Na początku ery Internetu we wczesnych latach 90. firewall pełnił rolę filtra bazującego na źródłowym i docelowym adresie sieciowym oraz tzw. porcie, czyli po prostu identyfikatorze aplikacji sieciowej. Przykładowe reguły systemu firewall mówiły np: "*zezwalaj wszystkim komputerom w sieci wewnętrznej na korzystanie z WWW; nie zezwalaj na wysyłanie danych do innych usług; nie zezwalaj na jakikolwiek ruch wchodzący do naszej sieci, poza protokołem e-mail do serwera obsługujacego pocztę*". W ciągu niecałych 10 lat okazało się, że takie rozwiązanie jest niewystarczające: przykładowo – zezwolenie na korzystanie użytkownikom z serwerów WWW oznacza, że mogli oni przy okazji pobrać z sieci różnego rodzaju mallware. Z kolei dopuszczenie ruchu e-mail do serwera poczty oznacza, że otwieramy drogę do wszelkiego radzaju zagrożeń

przesyłanych w załącznikach pocztowych. Odpowiedzią na ten problem było wprowadzenie na początku lat 2000. tzw. firewalli **UTM – "Unified Threat Management"** – co można przetłumaczyć niezbyt szczęśliwie jako "ujednolicone zarządzanie zagrożeniami". Systemy UTM dołączyły do typowego systemu firewall funkcje pełnione poprzednio przez autonomiczne, wyrafinowane (na owe czasy) i drogie systemy wykrywania i zapobiegania włamaniom (IDS/IDP), skanery antywirusowe oraz inne, np. skanery poczty elektronicznej. Firewall UTM stał się więc uniwersalnym "kombajnem" realizującym wszystkie funkcje bezpieczeństwa. Rozwój systemów UTM był milowym krokiem w dziedzinie bezpieczeństwa sieciowego, gdyż znacząco obniżył koszty – użytkownicy otrzymali "pudełkowe" rozwiązanie realizujące wszystkie możliwe funkcje bezpieczeństwa i to w dość umiarkowanej cenie. Systemy UTM są sprzedawane i wdrażane do tej pory, jednak stopniowo ustępują wprowadzonym pod koniec pierwszej dekady naszego wieku systemom **NGFW (Next Generation Firewall**, czyli po prostu - "firewall nowej generacji"). NGFW realizuje w zasadzie te same funkcje co UTM, jednak w inny sposób. O ile UTM jest systemem modularnym, w którym każda funkcja realizowana jest osobno, tj. przez odrębny dedykowany moduł, o tyle w NGFW cały przechodzący przez firewall ruch sieciowy poddawany jest kompleksowej analizie pod kątem wszystkich zagrożeń na raz. Przekłada się to na znaczne zwiększenie wydajności rozwiązania i tym samym zmniejszenie kosztów. NGFW mają też drugą dodatkową przewagę nad rozwiązaniami UTM: są w stanie efektywnie analizować i filtrować dane aplikacji WWW. Co to oznacza? Obecnie w dobie aplikacji internetowych oraz rozwiązań chmurowych bardzo wiele aplikacji korzysta z technologii WWW; przykładowo: poczta elektroniczna Gmail, Facebook, różnego rodzaju komunikatory, Youtube, bankowość elektroniczna i wiele innych – wszystko to są aplikacje, z których korzystamy za pomocą przeglądarki internetowej, wykorzystujące te same technologie, ale służące diametralnie różnym celom. Przykładowo – chcielibyśmy w polityce bezpieczeństwa zawrzeć następujace reguły: "*Pracownicy mogą bez przeszkód korzystać z firmowych kont pocztowych dostępnych przez WWW, oglądanie filmów z YT powinno być dozwolone tylko dla pracowników działu marketingu, Facebook powinien być zablokowany, dopuszczone jest korzystanie z komunikatorów*" ale bez możliwości przesyłania plików. Tego typu reguły bez problemu zrealizujemy przy pomocy systemu NGFW.

2. Jakie inne funkcje może pełnić firewall?

VPN czyli wirtualna sieć prywatna (Virtual Private Network) to technologia pozwalająca na łączenie użytkowników oraz całych oddziałów z centralą firmy w jedną logiczną sieć – za pośrednictwem sieci Internet. Komunikacja ta jest bezpieczna, gdyż cały transfer danych jest szyfrowany. Technologia VPN pozwala np. na "zanurzenie" sieci oddziałowych w sieci centrali, tak jakby fizycznie jej użytkownicy byli podłączeni do tej samej sieci lokalnej. VPN może pracować w dwóch głównych trybach:

- **Client-to-Site** – służy do połączenia indywidualnych użytkowników, np. pracujących w domu lub w "terenie".
- **Site-to-Site** – pozwala na łączenie oddziałów z centralą (lub kilku równorzędnych ośrodków) w jedną sieć.

Współczesne systemy firewall, jako że ze swojej natury stanowią pomost między siecią publiczną a prywatną, prawie zawsze pozwalają na realizację funkcji VPN. Jednocześnie, w wielu przypadkach są w stanie poddawać ruch VPN dodatkowej kontroli oraz separować w pewnym stopniu użytkowników VPN od pozostałych – przykładowo – nie chcielibyśmy, aby do sieci firmowej łączył się pracownik z komputera domowego, który został zawirusowany.

Deszyfracja ruchu jest funkcją, którą niejako wymusili dostawcy usług internetowych i usług "chmurowych" – obecnie już ponad połowa ruchu sieciowego usług WWW jest szyfrowana. Oznacza to, że standardowy firewall nie może poddać ich jakiekolwiek filtracji, najwyżej może je zablokować, co jest wylaniem dziecka z kąpielą. Przykładowo – jeśli ruch do chmurowego serwisu plikowego typu Dropbox, google-drive, itp. jest szyfrowany, to firewall nie jest w stanie wykryć wirusa w pobieranym pliku. Funkcja deszyfracji SSL pozwala na rozwiązanie tego problemu: zaszyfrowany transfer jest rozszyfrowywany tylko wewnątrz firewalla, analizowany i ponownie szyfrowany. Technologia ta jest skuteczna, ale obciążająca dla systemu firewall i w związku z tym ciągle dość kosztowna.

CC
Otwarte Systemy
Komputerowe Sp. z o.o.

ul. Rakowiecka 36, 02-532 Warszawa
tel. +48 22 646-68-73; fax +48 22 606-37-80
e-mail sales@cc.com.pl

Więcej informacji znajdziecie Państwo
w Internecie, na stronach
http://www.cc.com.pl

Kontakt:
Kontakt ogólny: cc@cc.com.pl
Dział Handlowy: sales@cc.com.pl
Dział Technizny: tech@cc.com.pl

Separacja stref i filtracja wewnętrzna

Separacja sieci wewnętrznej od sieci Internet jest kluczowym, ale nie jedynym zadaniem dla systemu firewall. Firewall może także posłużyć do realizacji filtracji sieciowego ruchu wewętrznego, tj. nie opuszczającego sieci danej organizacji. Obecnie przyjmuje się, że tylko w bardzo niewielkich i jednocześnie nieskomplikowanych pod względem IT organizacjach struktura sieci jest "płaska": tj. wszystkie komputery znajdują się w jednej sieci lokalnej i wzajemnie się "widzą". Dobre praktyki bezpieczeństwa mówią co innego: sieć komputerowa powinna być podzielona na podsieci zróżnicowane funkcjonalnie. I tak np. w typowej firmie produkcyjnej jako odrębne sieci logiczne powinny być wydzielone: komputery biurowe, komputery, z których odbywa się bezpośrednie zarządzanie produkcją, zaś maszyny i urządzenia sterowane cyfrowo powinny być także zlokalizowane w odrębnej podsieci. Podobnie w osobnej podsieci powinny znajdować się serwery wewnętrzne oraz serwery świadczące usługi zewnętrzne, np. sklep internetowy, system składania zamówień, itp., w osobnym segmencie sieci powinna znajdować się też sieć Wi-Fi (zwłaszcza jeżeli zapewnia ona dostęp gościom i osobom niebędącym pracownikami). Ponieważ komunikacja między rozdzielnymi segmentami jest jednak konieczna, rolę bramy pomiędzy nimi pełni właśnie system firewall.

Subskrybcje

Nabywając system firewall musimy zdawać sobie sprawę z tego, że zapewne nie będzie to wydatek jednorazowy. Współczesne systemy bezpieczeństwa IT (nie tylko firewall) w coraz większym stopniu polegają na stale aktualizowanej bazie zagrożeń, którą system sam aktualizuje poprzez sieć. Faktycznie, jakość danego rozwiązania i stopnień bezpieczeństwa, jaki on zapewnia, w coraz większym stopniu zależy od jakości bazy zagrożeń. Producenci systemów firewall udostępniają bazy w postaci odpłatnej subskrybcji (podobnie jak np. producenci systemów antywirusowych). Koszt rocznej subskrybcji może wahać się między 10% a 30% kosztów nowego rozwiązania. Zdarzaja się jednak przypadki, i są one coraz częstsze, w których całe rozwiązanie firewall dostępne jest jako subskrybcja. Producenci w różny sposób "konfekcjonują" subskrybcje baz bezpieczeństwa. Obecny trend polega na ich uproszczeniu, tak więc o ile kilka lat temu, w przypadku niektórych produktów możliwe było wykupienie nawet do 10 różnych subskrybcji, obecnie ich liczba jest ograniczana. Typowe subskrybcje to np.:

- **Baza zagrożeń** – obejmująca całokoształt znanego oprogramowania mallware, odpowiada w pewnym zakresie subskrybcji antywirusowej, jej rola jest jednak znacznie szersza.
- **Baza adresów WWW** – obejmuje znane serwisy WWW (zazwyczaj kilka- kilkadziesiąt milionów) poklasyfikowane według kategorii, pozwala na zablokowanie dostępu do określonych typów serwisów.
- **Baza antyspam** – firewall może pełnić rolę systemu antyspam, tj. usuwającego niechciane wiadomości z poczty elektronicznej, usługa taka zwykle realizowana jest na zasadzie odpłatnej subskrybcji.
- **Usługa "0-day"** – stosowana przez niektórych producentów – jest to specyficzna subskrybcja obejmująca dostęp do usługi producenta, która pozwala na wykrywanie zagrożeń "nieznanych", czyli takich, które pojawiły się w ciagu ostatnich minut i godzin, dla których nie opracowano jeszcze "szczepionki".

Powyżej wymieniliśmy tylko najbardziej typowe subskrybcje, u różnych producentów spotykamy się z różnorodnymi wariantami. Dodatkowo, szczególnie w przypadku firewalli sprzętowych, musimy też liczyć się z koniecznością wykupienia usługi gwarancyjnej oraz wsparcia na podstawowe oprogramowanie firewalla (zazwyczaj około 10-20% wartości rozwiązania rocznie).

3. Czym kierować się wybierając system firewall?

Przystępując do wyboru systemu firewall musimy zdawać sobie sprawę z głównych czynników różnicujących dostępne na rynku rozwiązania. Producenci zarzucają nas tabelkami zawierającymi dziesiątki parametrów oraz sloganami reklamowymi – na co należy zwrócić uwagę?

CC
Otwarte Systemy
Komputerowe Sp. z o.o.

ul. Rakowiecka 36, 02-532 Warszawa
tel. +48 22 646-68-73; fax +48 22 606-37-80
e-mail sales@cc.com.pl

Technologia – jak wcześniej wspomniano, na rynku dostępne są obecnie rozwiązania klasy UTM oraz NGFW. O ile nasza działalność faktycznie tylko w niewielkim stopniu bazuje na IT i nie przewidujemy znaczącego rozwoju naszej struktury informatycznej w ciągu kilku najbliższych lat, wskazany może być wybór nieco tańszego i prostszego rozwiązania UTM, w pozostałych przypadkach należy rozważyć wybór systemu NGFW.

Wydajność – głównym czynnikiem mającym wpływ na cenę rozwiązania firewall jest jego przepustowość, tj. mierzona w Megabajtach (lub Gigabajtach) na sekundę maksymalna wydajność filtracji ruchu sieciowego. Musimy pamiętać, że podawana przez producenta wydajność dotyczy calego systemu filtracji, tak więc jeśli posiadamy łącze internetowe o przepustowości 100 Mbps oraz chcemy także poprzez firewall przesyłać ruch do kluczowego serwera, dla którego maksymalną przepustowość ustaliliśmy na 100 Mbps (w obydwie strony, tj. jednocześnie z i od serwera) potrzebujemy rozwiązania o przepustowości ponad 300 Mbps. Musimy pamiętać, że cena firewalla oraz koszt jego utrzymania w kolejnych latach będzie głównie zależała od wydajności, tak więc parametru tego nie należy też przeszacować.

Oferowane na rynku rozwiązania dostępne są w dwóch odmianach: jako rozwiązania zintegrowane -sprzętowo-programowe, czyli "pudełkowe" oraz jako oprogramowanie, które zainstalować można na serwerze PC. Trudno jest jednoznacznie wskazać przewagę danego rozwiązania, gdyż wszystko zależy od wielu czynników. Rozwiązania zintegrowane są z całą pewnością prostsze w utrzymaniu, perspektywa posiadania tylko jednego sprzętowo-softwarowego komponentu jest bardziej atrakcyjna. Z drugiej strony należy pamiętać , że rozwiązanie zintegrowane posiada znaczące ograniczenia: producenci konkurując na rynku starają sie zaoferować możliwie niskie ceny, rozwiązanie pudełkowe może więc mieć znaczące ograniczenia wydajnościowe, zazwyczaj nie jest też możliwa jego rozbudowa (np. zwiększenie liczby interfejsów sieciowych). Rozwiązania zintegrowane dysponują niewielką pamięcią, nie jest więc, bez dodatkowych zewnętrznych serwerów możliwe gromadzenie informacji historycznych np. w celu realizacji analizy, prezentacji statystyk, itp.

4. Jaki system wybrać?

Kupując system firewall stajemy przed dość trudnym wyborem: na polskim rynku obecnych jest ponad dwudziestu producentów oferujących tego typu rozwiązania, w tym około 5-6 będących faktycznymi światowymi liderami branży. Ceny rozwiązania firwall są niebagatelne, dodatkowo musimy liczyć się z corocznymi opłatami subskrybcyjnymi związanymi z jego utrzymaniem.

Wybierając system firewall powinniśmy w programie minimum określić strategię rozwoju IT firmy w perspektywie 2-3 lat, poznać aktualne i przyszłe potrzeby oraz określić podstawowe założenia dotyczące polityki bezpieczeństwa. Pytania, na które powinniśmy znać odpowiedzi to:

1. Jaka jest liczba użytkowników naszej sieci, zarówno stacjonarnych jak i mobilnych (korzystających z sieci Wi-Fi)?
2. Czy wewnątrz firmy znajdują się serwery udostępniające usługi na "zewnątrz": serwer WWW, e-sklep, serwer poczty elektronicznej, itd?
3. Jeśli firma posiada oddziały, to jakie jest zapotrzebowanie oddziałów na serwisy zlokalizowane w centrali, np. czy oddziały korzystają z centralnego, firmowego serwera plików? Jaki ruch sieciowy sumarycznie generują oddziały?
4. Czy nasi pracownicy pracują zdalnie? Jeśli tak, to w jakim zakresie korzystają z firmowych zasobów IT? Jaki ruch sieciowy sumarycznie generują pracownicy zdalni?
5. Jaka jest przepustwość łącza internetowego w siedzibie (oraz w oddziałach), jak może się zwiększyć w ciągu najbliższych kilku lat? W jakim stopniu łącze jest faktycznie wykorzystane?
6. Jak krytyczne są funkcje IT w naszej firmie, jakie są koszty jednodniowego "przestoju" krytycznych systemów IT? Jaki jest koszt utraty danych przechowywanych na firmowych serwerach?

Pytania 1 i 5 pozwalają określić parametry wydajnościowe systemu firewall. Pytanie 2 dotyczy realizacji dodatkowej filtracji i wydzielenia dodatkowych stref bezpieczeństwa. Pytania 3 i 4 pozwalają określić, czy jest zapotrzebowanie na bramkę VPN, w jakim trybie będzie ona pracować i jaka jest jej wymagana wydajność. Pytanie 6 pozwala przeprowadzić zgrubną analizę ryzyka – jeśli przedsiębiorstwo w małym stopniu polega na systemach IT, np. realizując outsourcing usług

CC
Otwarte Systemy
Komputerowe Sp. z o.o.

ul. Rakowiecka 36, 02-532 Warszawa
tel. +48 22 646-68-73; fax +48 22 606-37-80
e-mail sales@cc.com.pl

Więcej informacji znajdziecie Państwo
w Internecie, na stronach
http://www.cc.com.pl

Kontakt:
Kontakt ogólny: cc@cc.com.pl
Dział Handlowy: sales@cc.com.pl
Dział Technizny: tech@cc.com.pl

takich jak księgowość i nie posiada cennych danych, być może jest w stanie pozwolić sobie na poważniejsze zakłócenia w tym obszarze. W firmach polegających w większym stopniu na technologii IT nawet kilkugodzinna przerwa w dostępie do sieci oraz wewnętrznych systemów może oznaczać bardzo poważne straty – w takim przypadku warto zainwestować więcej w system firewall.

Jak już wspomniano, decydujący wpływ na cenę ma przepustowość systemu firewall. Jednak podawane przez producentów dane mogą łatwo wprowadzać w błąd. Przyjrzyjmy się danym podawanym przez jednego z producentów dla systemu przeznaczonego na rynek małych firm:

Nr	***Parametr***	***Przepu-stowość***
1	Przepustowosć maksymalna	1.3 Gbps
2	Przepustowość VPN	200 Mbps
3	Przepustowosć przy filtrowaniu SSL	210 Mbps
4	Przepustowość przy filtrowaniu zagrożeń	190 Mbps

Z pozoru maksymalna przepustowość podana w poz. 1 powinna zaspokoić ponad miarę potrzeby nawet wymagających użytkowników: rzadko kiedy dysponować będziemy łączem internetowym o szybkości realnie zbliżonej do 1 Gbps. Jednak już przepustowość usług VPN (poz.2) jest znacząco niższa: całkowity ruch połączeń szyfrowanych dla oddziałów i zdalnych użytkowników nie może przekroczyć 200 Mbps. Podobnie - jeśli zdecydujemy się na deszyfrowanie ruchu SSL, przepustowość wyniesie tylko około 200 Mbps (poz. 3). Przy pełnym filtrowaniu zagrożeń (a więc funkcje wykrywania mallware'u, itd.) przepustowość jest nawet niższa od 200 Mbps. Należy jednak zwrócić uwagę na to, czego ten producent nie podaje (i czego z reguły nie podają producenci w danych technicznych) – każdy z w.w. parametrów wydajnościowych mierzony jest oddzielnie w wyidealizowanych warunkach i dla nieaktywnych pozostałych funkcji bezpieczeństwa. Nie wiemy np. jaka będzie przepustowość tego systemu przy: włączonej deszyfracji ruchu SSL, z włączonym wykrywaniem wszystkich zagrożeń i przy np. 50% udziale ruchu VPN! Możemy się jednak spodziewać, że będzie dużo niższa, zapewne na poziomie 30-50 Mbps – to już znacząco poniżej przepustowości oferowanych obecnie łączy internetowych. Przy 25-40 użytkownikach daje nam to 1-2 Mbps na użytkownika korzystającego z Internetu – to już znacząco poniżej poziomu komfortu, a pamiętajmy, że mówimy o całkowitej przepustowości, także dla ruchu wchodzącego np. generowanego przez oddziały, klientów, itp.
Tak więc, do specyfikacji producentów należy podchodzić krytycznie i bazować także na ocenach niezależnych firm specjalizujących się w ocenie rozwiązań IT (np. Gartner, czy NSSA Labs).

Na zakończenie – należy jednak pamiętać, że firewall jest najważniejszym, ale nie jedynym elementem "układanki", jaką stanowią systemy cyberbezpieczeństwa w firmie. Wrogie oprogramowanie może wniknąć do naszej sieci z jego pominięciem, np. poprzez pendrive. Firewall tylko w ograniczonym zakresie ochroni nas przed złośliwym czy też wynikającym z braku umiejętności zachowaniem pracowników związanym np. z kradzieżą czy nieautoryzowanym transferem krytycznych danych poza firmę. Firewall nie ochroni nas też przed dostępem do systemów wewnętrznych przez osoby niepowołane, które w przeszłości uzyskały odpowiednie poświadczenia, a którym zapomniano je odebrać (opisane są liczne przypadki szkodliwych działań byłych pracowników). Tak więc wybierajac system firewalll musimy pamiętać też o innych elelementach systemu zabezpieczeń: ochronie komputerów PC i indywidualnych serwerów, szyfrowaniu danych, dodatkowej autoryzacji użytkowników, ochronie sieci Wi-Fi oraz ochronie i monitorowaniu dostępu zdalnego.

Notka autorska:

Grzegorz Blinowski jest adiunktem w Instytucie Informatyki Politechniki Warszawskiej, zajmuje się tematyką systemów rozproszonych i bezpieczeństwem sieci komputerowych. Jest autorem kilkudziesięciu publikacji naukowych oraz dwóch książek poświęconych tematyce IT. Był także promotorem ponad czterdziestu prac magisterskich i inżynierskich. Posiada certyfikat CISSP. Jest też założycielem spółki informatycznej "CC" zajmującej się usługami w zakresie bezpieczeństwa sieci i systemów. Artykuł w skróconej postaci ukazał się w 2018 r. w „Paradniku Biznesu" Media Planet w ramach dodatku do gazety *Rzeczpospolita*.