CZY MOGĘ BYĆ BEZPIECZNY W SIECI INTERNET?

KOMAKO

Czy mogę być bezpieczny dzisiaj w sieci Internet ?

TAK !

Nie od dziś wiadomo, że każdy, kto ma dostęp do poufnych informacji w wersji elektronicznej może stać się celem cyberprzestępców. Informacje takie jak te dotyczące kont bankowych czy dane osobowe mogą wzbudzić niepożądane zainteresowanie niezależnie od wielkości Twojej firmy.

Co więcej, małe firmy często są bardziej atrakcyjne dla hackerów, ponieważ zdarza się, że mają słabsze zabezpieczenia niż te większe organizacje.

Połączenie w jedną całość nowych pracowników, biur, urządzeń i aplikacji stanowi wyzwanie dla rozwijającej się firmy. Żeby dalej napędzać jej rozwój, trzeba zrobić to łatwo, bezpiecznie i w ramach rozsądnego budżetu.

Niezależnie od tego, na jakim etapie rozwoju znajduje się firma, Fortinet ma wszystko, czego potrzeba, by pomóc naszej firmie w dalszej drodze — najwyżej oceniane zabezpieczenia klasy korporacyjnej chroniące wszystko od połączenia internetowego po urządzenia użytkowników końcowych, dostęp przewodowy i bezprzewodowy oraz najbogatszą ofertę dodatkowych rozwiązań bezpiecznej komunikacji i ochrony aplikacji — a to wszystko łatwo zarządzane z jednej konsoli.

Małe firmy są celem zawsze

Małe firmy zazwyczaj nie używały funkcji zabezpieczeń często stosowanych w większych przedsiębiorstwach głównie ze względu na ich koszty i złożoność. Naruszenia bezpieczeństwa danych coraz częściej występują jednak w mniejszych organizacjach, czy to ze względu na same dane czy na dostęp do większych przedsiębiorstw, jaki mogą one zapewniać. Według raportu Data Breach Incident Report firmy Verizon naruszenia bezpieczeństwa danych częściej występowały w małych niż w dużych organizacjach.

Czy wiesz, że :

- **25% naruszeń bezpieczeństwa miało miejsce w małych firmach**
- **74% małych firm zezwala na używanie prywatnych urządzeń do celów służbowych**
- **co drugi pracownik z pokolenia Y naruszyłby zasady korzystania z własnych urządzeń do celów służbowych**

W bardzo młodych firmach często używa się urządzeń biurowych działających na zasadzie plug-and-play, jak również podstawowych usług głosowych, pocztowych i innych świadczonych przez menedżera obiektu lub usługodawcę internetowego. Chociaż łatwo jest je włączyć przy minimalnych kosztach początkowych, w miarę rozwoju firmy takie miesięczne opłaty za usługi zaczynają się kumulować, aż po jakimś czasie bardziej opłacalne dla wielu organizacji okazuje się wdrożenie własnych systemów działających na miejscu, które są zarówno tańsze, jak i bardziej skalowalne i łatwiejsze w obsłudze.

Czy wiesz, że :

- **38% naruszeń bezpieczeństwa było spowodowane lukami w zabezpieczeniach aplikacji**
- **23% odbiorców otwiera wiadomości wyłudzające informacje, a 11% klika w załączniki**

W obecnych czasach życie prywatne i zawodowe się przenikają – korzystamy ze służbowych telefonów, laptopów, obsługujemy firmowe konta także poza godzinami pracy. Często przez 24 godziny na dobę pod naszą pieczą jest sprzęt oraz hasła do różnego rodzaju systemów, w tym m.in. systemów bankowych. W świecie nowoczesnych technologii hasła internetowe mają taką samą wartość jak klucze czy portfel. Wystarczy utrata jednego z nich, by narazić się na przykre konsekwencje, które mogą dotknąć także naszej sfery zawodowej. W związku z tym powinniśmy podwoić naszą czujność – **jesteśmy odpowiedzialni nie tylko za prywatne, ale i służbowe dane i zasoby.**

Jeśli zarządzamy dużą ilością loginów i haseł dobrym, zalecanym rozwiązaniem jest korzystanie z oferowanego przez renomowanego producenta menedżera haseł. Jest to jednocześnie efektywna, jak i bezpieczna metoda. Nie zwalnia nas to jednak z zachowania czujności oraz okresowej zmiany hasła dostępowego do programu. **Zdecydowanie złym pomysłem jest natomiast zapisywanie wszystkich haseł w plikach tekstowych na komputerze**, uaktywnianie opcji zapamiętywania haseł, czy też autologowania (także w przypadku serwisów zawierających bardzo wrażliwe dane!). Może i w ten sposób ułatwiamy swoją pracę, jednak odbywa się to kosztem naszego bezpieczeństwa teleinformatycznego.

Sprawia to, że w przypadku utraty sprzętu (co również jest możliwe, ze względu na fakt, że często pozostawiamy go pozbawionego należytej ochrony) lub przeprowadzenia zdalnego ataku, grozi nam ogromne ryzyko, którego konsekwencje mogą być bardzo poważne.

Czy wiesz, że :

- **82% wszystkich „zarażeń" następuje w ciągu minut, od uruchomienia elementu niepożądanego (np. załącznika w mailu)**
- **11% zarażeń następuje w ciągu sekund**
- **6% zarażeń występuje w ciągu kilku najbliższych godzin**

Jakość rozwiązań ochronnych (brzegowych), które zadziałają w sposób niemal natychmiastowy, jeszcze zanim kod niepożądany dotrze do potencjalnej ofiary, **jest kluczowa do ochrony zasobów lokalnych**.

Zgodnie z zasadą :

im taniej, tym gorzej

należy zmienić optykę patrzenia na zabezpieczenia brzegowe wyłącznie poprzez cenę, a naprawdę, skupić się na szybkości działania i skuteczności takich rozwiązań.

Na rynku dostępny jest obecnie szeroki wybór programów chroniących użytkowników przed złośliwym oprogramowaniem oraz atakami hakerów. Jednak aplikacja lokalnie działająca, nie zapewni nam pełnego bezpieczeństwa, jeżeli sami nie będziemy ostrożni podczas przeglądania zasobów Internetu czy obsługiwania poczty e-mail. Coraz częściej bowiem hakerzy do włamań zamiast skomplikowanych skryptów i algorytmów, wykorzystują socjotechnikę, bazując na **ludzkiej naiwności, pośpiechu oraz braku wiedzy w zakresie bezpieczeństwa informatycznego**.

Zawartość elektroniczna otrzymywanych informacji też jest groźna

Wszystkie dokumenty otrzymywane w załącznikach, a kierowane na służbowe adresy maili, w **78% są fałszywymi danymi**, mającymi za zadanie przejęcie komputera (załączniki PDF, DOC, XLS, JPG, GIF, PNG i wiele innych). Nie należy otwierać plików zip/rar/itp. przesyłanych e-mailem i spakowanych na hasło (gdzie hasło jest podane w treści e-maila). Dotyczy zarówno wezwań do zapłaty, listów przewozowych z DHL i awizo z Poczty Polskiej, jak i szeregu innych "pomysłów" na jakie wpadną w najbliższych dniach przestępcy. Jest to najbardziej popularny sposób infekcji tzw. bankerami, czyli złośliwym oprogramowaniem odpowiedzialnym za podmianę numeru rachunku podczas zlecenia przelewu.

Dla wielu pracowników, otwieranie załączników i przeszukiwanie Internetu jest częścią ich pracy, przez co trudniej jest zachować czujność. Dzisiejsze ataki phishing są dużo bardziej wiarygodne i podstępne niż kiedyś. Ukierunkowany phishing, wykorzystuje dane internetowe i profile mediów społecznościowych, aby dostosować atak względem ofiary. Otwieranie nieoczekiwanych faktur lub ważnych wiadomości bankowych, bez wcześniejszego upewnienia się co do wiarygodności otrzymanej wiadomości, jest często skutkiem ludzkiej ciekawości. **Przeciętny użytkownik uważa, że kwestia bezpieczeństwa jest pracą kogoś innego i nie leży w jego obowiązkach.**

Przestępcy przeważnie podszywają się pod znane firmy, instytucje publiczne, partnerów biznesowych lub współpracowników. Najczęściej w tym celu wykorzystywane są adresy e-mail łudząco podobne do prawdziwych. W treści maila zazwyczaj umieszczane są linki lub dokumenty, które po otwarciu automatycznie kierują użytkownika na stronę ze złośliwym oprogramowaniem czy niepostrzeżenie pobierają aplikację umożliwiającą włamanie do komputera. Może się również zdarzyć, że malware zostanie ukryty w pozornie bezpiecznym pliku – np. kilkuset stronicowej instrukcji obsługi w formacie PDF i nie będzie dla nas widoczny na pierwszy rzut oka. W efekcie nim spostrzeżemy, że coś jest nie tak, w naszym systemie zostaną dokonane nieodwracalne zmiany (komputer jest przejęty przez bootnet).

Czy wiesz, że :

- **najbardziej popularne hasła w 2015 roku :**
  - **123456**
  - **password**
  - **12345**
  - **12345678**
  - **qwerty**
- **aż 73% kont typu on-line, jest zabezpieczonych zduplikowanym hasłem (tym samym)**
- **54% osób używa 5 lub mniej haseł we wszystkich kontach typu on-line, z których korzysta (!!)**
- **średnio 6 różnych haseł, zabezpiecza 24 konta typu on-line (czyli 4 konta typu on-line są zabezpieczone tym samym hasłem – przez różne osoby)**

Niestety, w dobie ciągłego pospiechu i nadmiernej ufności wobec zasobów sieci Internet, **ataki bazujące na socjotechnice odnoszą coraz większy sukces**. W ten sposób narażamy się na utratę cennych danych lub poważne straty finansowe, zagrażając naszej karierze czy funkcjonowaniu całej firmy.

Czy wiesz, że :

- **w roku 2015, 2-ch na 5 ludzi na tej planecie, miało styczność z przynajmniej 3-ma formami kompromitacji swojej tożsamości :**
  - **zablokowane konto w banku, pocztowe itp.**
  - **hasło zostało ujawnione w wyniku działań hackerskich**
  - **otrzymało informacje, że swoje dane osobiste, zostały ujawnione (np. z mediów socjalowych, prasy, instytucji itp.)**
- **tylko 2 osoby na 10, żywotnie interesuje się swoim bezpieczeństwem w dostępie do kont typ on-line**
- **7 osób na 10 nie interesuje się, zabezpieczeniem swoich danych w usługach typu on-line (lub nie wie jak, lub nie ma możliwości)**
- **21% osób używa tych samych haseł przez 10 lat (!!)**
- **47% osób używa haseł starszych niż 5 lat (!!)**

Jak zatem ustrzec się przed tego typu atakami?

Przede wszystkim nie spieszmy się podczas przeglądania wiadomości e-mail.

Uważnie czytajmy treść, a za nim otworzymy załączony plik lub klikniemy w przesłany link, zweryfikujmy nadawcę. Jeśli pojawi się jakikolwiek cień wątpliwości – w żadnym wypadku nie otwierajcie żadnego załącznika – od razu należy takiego maila skasować {Shift-Delete}.

Nie zaszkodzi również, jeżeli przeskanujemy otrzymaną wiadomość pod kątem obecności szkodliwego oprogramowania. I najważniejsze, jeśli coś wzbudzi nasze wątpliwości, niezwłocznie zgłośmy się do firmowego działu IT.

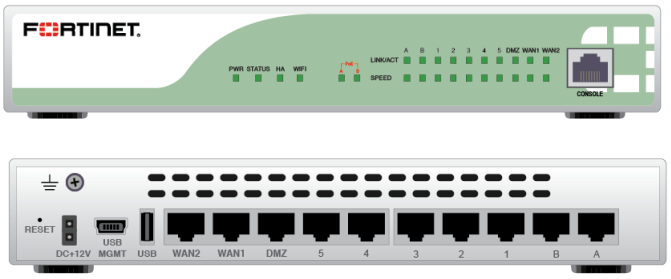
Ograniczenie aktywności w zasobach społecznościowych – głównego źródła rozprzestrzeniania się kodu złośliwego, a także pozyskiwania wszelkich – zaznaczamy, wszelkich informacji o sobie samym, firmie, o innych, jest oczekiwanym podejściem do ochrony swojej tożsamości, swoich danych osobowych, a w konsekwencji również swojego życia społecznego.

Czy wiesz, że :

- **Twój biznes, Twoja praca, Twoja tożsamość, jest zależna od innych ?**
- **86% firm w USA i Kanadzie sprawdza, czy partner biznesowy, jest na odpowiednim poziomie chroniony, aby nie spowodował jakiś perturbacji w ich procesach biznesowych !!**

JAK się chronić ?

Jednym ze sposobów ochrony danych i całego środowiska IT w firmie (pracy, domu) są urządzenia UTM.



Są one idealne dla małych i średnich firm, bo są przystępne cenowo oraz w prosty sposób chronią sieć przed wirusami, malware czy cyberatakami, zawierają ochronę na wszystkich wymaganych poziomach. Potrzeby technologiczne małych biur rosną każdego roku i dlatego nie należy ryzykować utraty swoich cennych danych lub doprowadzać do możliwości wystąpienia sytuacji ryzykownej, w której następuje pojawienie się namacalnych start (np. utrata środków finansowych na koncie w banku).

W celu umożliwienia pracownikom korzystania z urządzeń przenośnych, wiele małych biur wdraża sieci bezprzewodowe i zezwala na używanie urządzeń prywatnych do celów służbowych (pracę w modelu BYOD) — rozwiązania, które dotychczas były stosowane w większych przedsiębiorstwach.

Te **nowe technologie nakładają nowe wymagania dotyczące bezpieczeństwa** danych i zgodności z przepisami. Każde urządzenie komunikujące się bezprzewodowo, powinno podlegać kontroli i sprawdzeniu, czy nie przenosi kodu złośliwego, co nie jest takie trudne, biorąc pod uwagę ilość np. złośliwych aplikacji w app-storach poszczególnych producentów platform (Google, Apple, Microsoft).

Czy wiesz, że :

- **ilość uruchomionych urządzeń bezprzewodowych tzw. IoT (the Internet of Things) do 2020 roku osiągnie 24mld sztuk**
- **urządzenia IoT nie posiadają żadnych mechanizmów ochronnych (np. bezprzewodowa szczoteczka do zębów)**
- **aktualnie, czas potrzebny na włamanie się do urządzeń IoT, wynosi ok 3 min.**

Urządzenia UTM są to rozwiązania, które integrują w sobie : firewall, wykrywanie intruzów (IPS), VPN, kontrola pasma (QoS), antywirus, antyspyware, antyspam, filtrowanie stron www i kontrola aplikacji (np. komunikatory i ruch P2P) oraz autentykację dostępu do zasobów.

Przewaga urządzeń UTM nad „zwykłymi" routerami xDSL

jest ogromna

– zwykłe routery nigdy nie posiadały (i nie będą) zaawansowanych technologii ochrony ruchu TCP/IP i zawartości, w znaczeniu ochrony np. AV (zanim ruch szkodliwy dotrze do stacji użytkownika jest już wiele razy sprawdzony na tym urządzeniu) .

Proponowane przez nas rozwiązanie do ochrony granicy LAN/WAN, jest propozycją, która w sposób kompleksowy obejmuje ochronę zasobów lokalnych, nie tylko na komputerach , ale przede wszystkim w momencie zanim pobierane zawartości trafią do konkretnego użytkownika w chronionej sieci LAN - **jest to kluczowa cecha tego rozwiązania**; zanim użytkownik sieci lokalnej otrzyma maila, pobierze treść w przeglądarce, odbierze informacje w komunikatorze, skopiuje pliki itp. zostaną te działania sprawdzone, a następnie w zależności od wyników weryfikacji udostępnione lub nie – ze stosownym komunikatem, że niestety drogi użytkowniku, nie możesz pobrać takiej czy innej zawartości, bo jest ona szkodliwa (i zablokowana).

Czy wiesz, że :

- **co roku, moc maszyn do łamania haseł podwaja się**
- **61% wdrożeń różnych technologii bezpieczeństwa, kończy się niepowodzeniem z powodu wymagań konfiguracyjnych (zbyt skomplikowane)**
- **55% firm zarejestrowało 6 lub więcej cyber-ataków lub prób przełamania zabezpieczeń w ciągu 12-mcy**

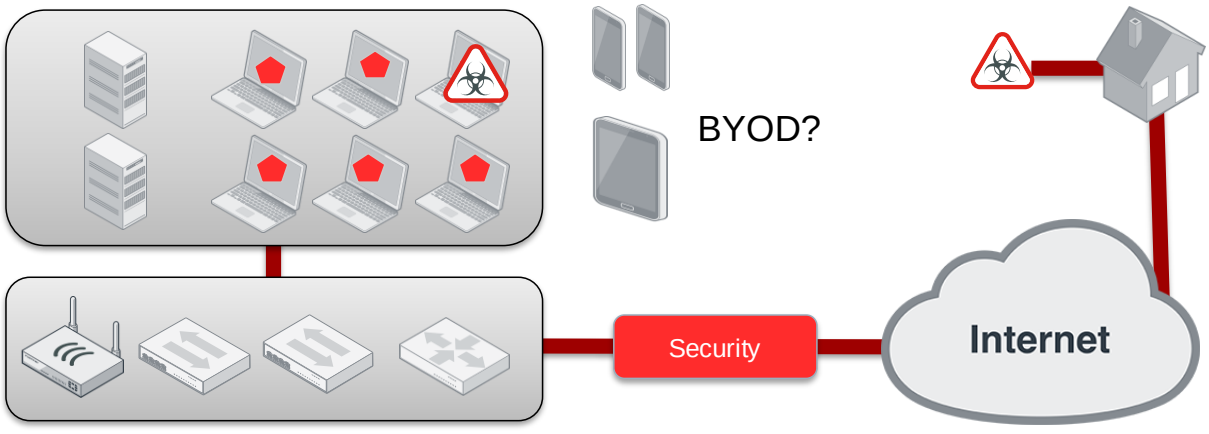
Mając tego typu rozwiązanie, jesteśmy na bieżąco wstanie kontrolować gdzie, kiedy, kto i co może wysłać (nie tylko maile się wysyła) z sieci lokalnej, a także, co, skąd, do kogo i częściowo w jakim celu wysyłane są dane z sieci lokalnej. **I to nie wszystko**, ponieważ również w tym rozwiązaniu mamy pełną paletę technologii służących do ochrony przed bezpośrednimi atakami (w zasadzie dowolnej postaci), na zasoby sieci lokalnej.

Stworzenie dobrej ochrony nie jest już takim łatwym i prostym zadaniem

W większości przypadków, ochrona typu AV to za mało (np. ruch generowany przez bootnety, albo skrypty wykonywane przez przeglądarki, służące wykradaniu danych dostępowych do witryn bankowości on-line).

Dzisiaj niezbędne jest użycie rozwiązań, które są

świadome treści przesyłanych do/od użytkownika sieci Internet.



Czy wiemy co się dzieje w naszych komputerach ?

Zaszyfrowany ruch SSL (np. witryny których adres zaczyna się od : *https://.....*), **nie może być skutecznie sprawdzony pod kątem zawartości niebezpiecznego kodu**, przy wykorzystaniu zwykłego skanera AV, jaki jest najczęściej używany na naszych komputerach lokalnych.

Czy wiesz, że :

- **85% ruchu w sieci Internet to komunikacja zaszyfrowana ? (i nie wiesz, co się w niej dzieje)**
- **tylko najwyższej klasy urządzenia UTM mogą bez utraty wydajności „zajrzeć" do środka komunikacji szyfrowanej i sprawdzić, czy nie ma tam zagrożenia dla nas**
- **90% mocy komputera lokalnego jest wykorzystywana na operacje sprawdzające ruch SSL – na resztę operacji nie ma więcej mocy (spadek wydajności)**

Wydaje się, że ta różnica w sposobie podejścia do ochrony AV w takim „tradycyjnym" modelu, sprawiająca niestety również wiele problemów w jej codziennej konserwacji, powoduje, że oczekiwany efekt końcowy nie dość, że miesza się z uczuciem niezadowolenia lub irytacji z powodu spadku wydajności komputerów, to jeszcze powoduje, że nie jest ona mimo wszystko tak szczelna jak byśmy sobie to zakładali czy oczekiwali (oraz skuteczna).

Dlatego do ochrony granicy LAN/WAN, komputerów lokalnych oraz użytkowników, proponujemy uruchomienie rozwiązania, które spowoduje, że sieć będzie chroniona, nie tylko w zakresie komputerów lokalnych, ale przede wszystkim sieć lokalna **jako cały organizm** – ruch pakietów, działania użytkownika i środowisko komputerów. Brak ochrony jednego z tych obszarów, powoduje, że całość środowiska IT nie jest w pełni chroniona.

W obecnych czasach działania sieci Internet, **urządzenia UTM są jedynym (jeszcze) skutecznym rodzajem ochrony**, który daje czas na podjęcie jakiś działań ochronnych przez użytkowników; często po infekcji chociażby takimi zagrożeniami jak diskcryptery (złośliwe szyfrowanie dysków zaatakowanego komputera, w celu wymuszenia okupu), po działaniu których nie ma w zasadzie co zbierać z danych. Bogata oferta firmy Fortinet pomaga wdrożyć, chronić i obsługiwać systemy poczty elektronicznej, komunikacji głosowej i łączności internetowej.

KOMAKO

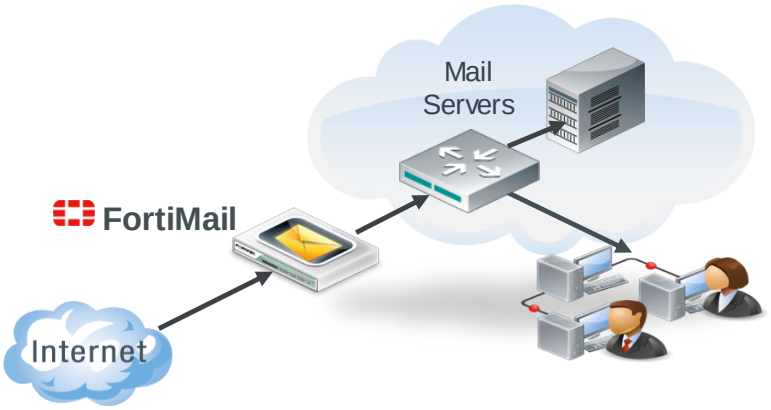
FORTINET
AUTHORIZED PARTNER

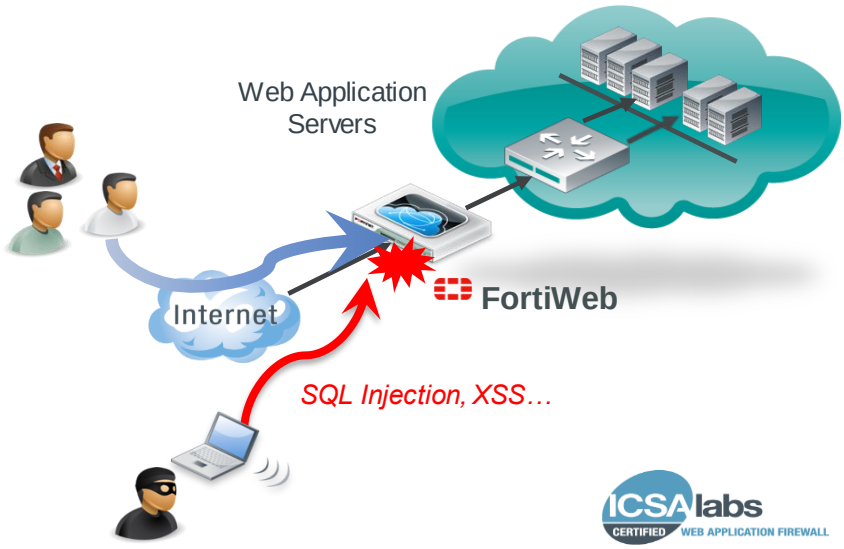
Jako wiodący producent i lider rozwiązań z zakresu ochrony UTM, firma

Fortinet

oferuje kompleksową ofertę, na jednolitą, wydajną i skuteczną ochronę danych cyfrowych w firmie, w pracy, w urzędzie, w domu, w szkole, w wielkim Data Center, w szpitalu, w przemyśle –

gdziekolwiek





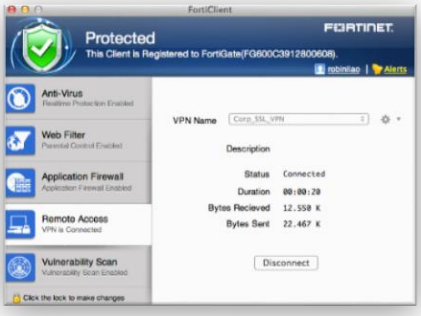
Obszar produktów firmy Fortinet pokrywa w całości potrzeby małych firm w zakresie bezpieczeństwa danych :

- **FortiGate** zintegrowane zarządzania zagrożeniami (obecnymi i przyszłymi) – podstawa systemu ochrony

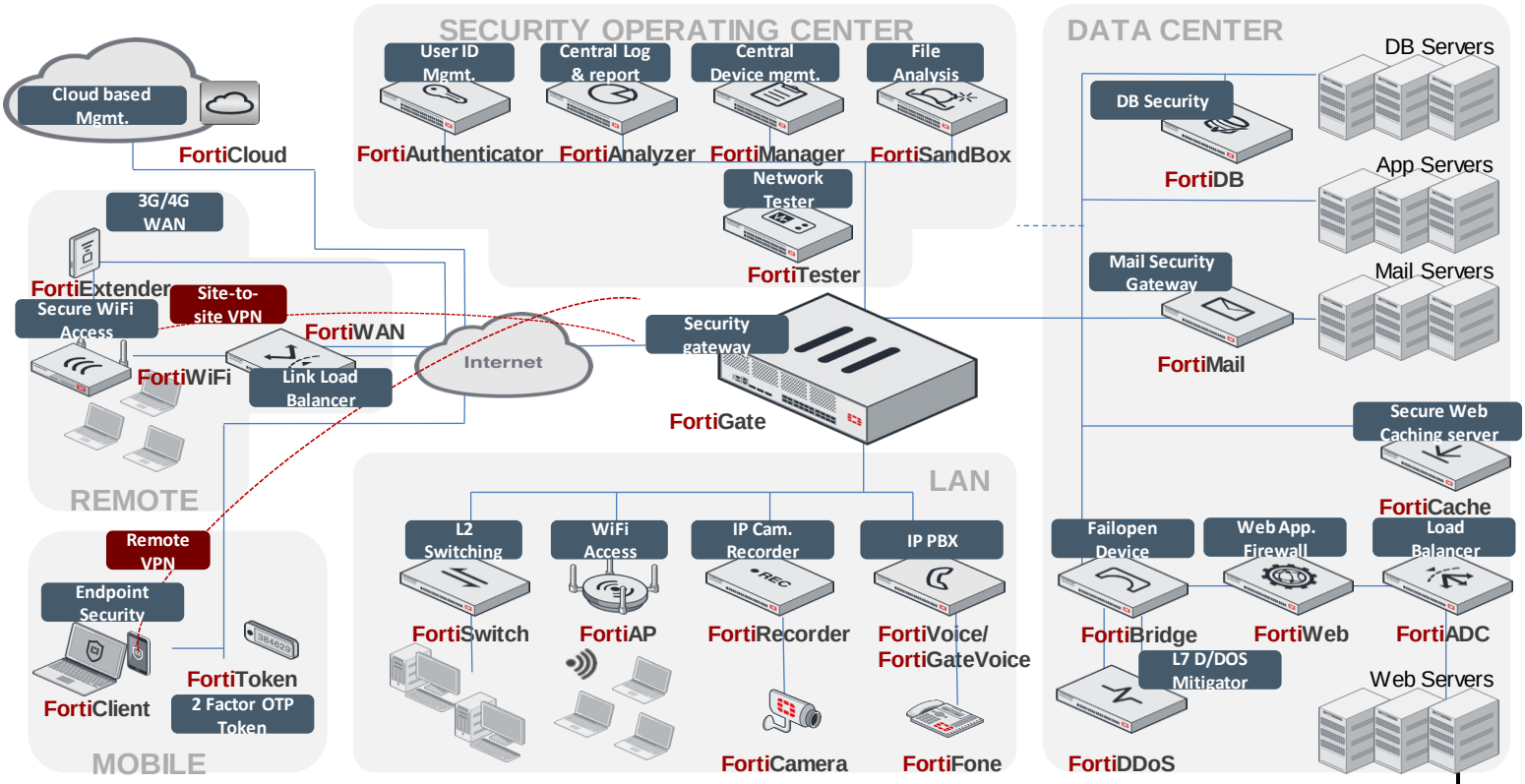
- **FortiAP** bezpieczne punkty dostępowe dla sieci bezprzewodowych WiFi

- **FortiSwitch** bezpieczna komunikacja wewnętrzna

- **FortiClient** zabezpieczenie punktów końcowych



- **FortiVoice** zabezpieczenie komunikacji głosowej VoIP (centrala PBX)
- **FortiMail** serwer i bezpieczeństwo poczty elektronicznej
- **FortiWeb** ochrona aplikacji internetowych



Jak widać na powyższym schemacie, wiemy co i jak zabezpieczyć.

Zaczynając od podstawy – **Security Gateway**, można stworzyć ochronę dla najważniejszych danych w naszej firmie. Mamy kontrole nad użytkownikiami, nad ruchem który jest przez nich generowany, możemy chronić połączenia komunikacje głosową w oparciu o protokół SIP (komunikatory, telefony VoIP), możemy zestawiać bezpieczne połączenia z zewnątrz firmy do zasobów lokalnych, chronimy wszystkie komputery firmowe, a jeśli jest taka potrzeba, to również komputery prywatne naszych pracowników, możemy włączyć monitoring – wiemy cokolwiek o zdarzeniach fizycznych (np. włamanie, kradzieże).

Czy wiesz, że :

- **67% wszystkich zarażeń, wykrywanych jest w dniach, co w zasadzie doprowadza do całkowitej utraty danych chronionych**
- **21% zarażeń, jest wykrywana w ciągu minut, co powoduje uszkodzenia w danych na poziomie 25-35% wszystkich chronionych danych; ta wartość w dużej mierze nie dotyczy rynku SMB, który ma bezwładność liczoną w dniach**
- **7% zarażeń, wykrywana jest w sekundach – głównie w segmencie Enterprise, który ma odpowiednie środki zainwestowane w skuteczną ochronę brzegową**
- **2,5% zarażeń wykrywanych jest w ciągu godzin – nie dotyczy rynku SMB**

Co mogę zrobić ?

Wiele. A przy użyciu odpowiedniego rozwiązania, niemal w całości można odsunąć zagrożenie tak daleko, jak to tylko możliwe.

[...Be like water my friend...]

Bruce Lee

Opracuj plan kopii zapasowych i odzyskiwania. Regularnie twórz kopie zapasowe systemów oraz przechowuj je na osobnym urządzeniu w trybie offline (dotyczy wszystkich bez wyjątków).

Korzystaj z profesjonalnych zabezpieczeń internetowych, takich jak urządzenia UTM firmy Fortinet oraz narzędzi pozwalających skanować zawartość e-maili, stron czy plików w poszukiwaniu szkodliwego oprogramowania.

Istotne jest również blokowanie potencjalnie niebezpiecznych reklam i witryn mediów społecznościowych, które nie mają znaczenia biznesowego. Narzędzia te powinny być wyposażone w funkcję piaskownicy (sandbox), dzięki czemu nowe lub nierozpoznane pliki mogą być analizowane i uruchamiane w bezpieczny sposób.

Aktualizuj swoje systemy operacyjne, urządzenia oraz oprogramowanie – tablety, smartphony, notebooki, komputery stacjonarne, skanery, drukarki, czytniki.

Upewnij się, że Twój antywirus, IPS i antymalware są uaktualnione do najnowszej wersji.

Jeśli to możliwe, korzystaj z białej listy, która zapobiega pobieraniu i uruchamianiu nieautoryzowanych aplikacji. Zalecane jest zastanowienie się, czy aby na pewno ta czy inna aplikacja jest mi naprawdę niezbędna ?

Podziel swoją sieć na strefy bezpieczeństwa, zapobiegając tym samym rozprzestrzenianiu się potencjalnej infekcji – wydziel w swojej sieci (w firmie, w domu, gdziekolwiek) sieć dla maszyn ważnych, istotnych, sieć dla urządzeń gości, którzy nas odwiedzają, sieć dla bezprzewodowych peryferii, które nie mają łatwo dostępnego interfejsu (IoT), sieć dla drukarek, skanerów itp.

Nadaj użytkownikom indywidualne prawa dostępu tak, aby potencjalnie jak najmniejsza ich liczba była w stanie zarazić dane, usługi czy aplikacje o krytycznym znaczeniu. Nie każdy musi pracować na koncie z uprawnieniami administracyjnymi. A im mniejsze uprawnienia, tym wyższa trudność dla potencjalnie szkodliwego kodu, na zmodyfikowanie środowiska i przejęcie go przez przestępców, agencje rządowe itd.

Wdróż rozwiązanie bezpieczeństwa BYOD odpowiedzialne za inspekcje i blokowanie urządzeń niespełniających wymogów bezpieczeństwa (np. za brak zainstalowanego klienta antymalware'owego, nieaktualna baza antywirusa lub brak kluczowych łatek w systemie operacyjnym nie wpuszczamy do naszych zasobów).

Korzystaj z narzędzi analitycznych, dzięki którym po ataku można określić :

- skąd pochodzi infekcja,
- jak długo była w danym środowisku,
- czy została usuniętą ze wszystkich urządzeń,
- czy infekcja nie powróci.

Uświadamiaj pracowników, znajomych i kogokolwiek innego w kwestiach bezpieczeństwa. Poinstruuj użytkowników, aby w e-mailach nie klikali w nieznane załączniki i linki oraz nie pobierali plików niewiadomego pochodzenia.

To człowiek jest najsłabszym ogniwem

łańcucha bezpieczeństwa i to na nim należy skupić uwagę i przedsięwziąć odpowiednie środki ochronne i zaradcze.

Czy wiesz, że :

- **z tego miejsca :**
  http://forticlient.com

  możesz pobrać i korzystać całkowicie bezpłatnie z profesjonalnego programu do ochrony lokalnego komputera (licencja nie wygasa, cały czas jest aktywna subskrypcja wzorców dla ochrony AV), zamiast korzystać z wątpliwej reputacji rozwiązań ?

Jak widać, należy sporo wykonać, aby stworzyć

swój własny, bezpieczny, cyfrowy świat

Zadanie nie jest proste, ale nie jesteście sami – **jesteśmy MY – profesjonaliści**, dysponujący dostępem do odpowiednich rozwiązań firmy Fortinet, które chcemy **dla Was uruchomić, pokazać, objaśnić i wyjaśnić.**

Niezbędnym warunkiem jest również korzystanie z

bezpiecznego kanału komunikacyjnego

jakim jest **profesjonalna usługa pocztowa**. Od niej w zasadzie wszystko się zaczyna.

Korzystanie z tanich, często bezpłatnych usługodawców poczty elektronicznej, bardzo szybko kończy się pojawieniem najprzeróżniejszych problemów :

- spam,
- niechciana poczta,
- ataki na swój własny serwer pocztowy,
- wirusy,
- reklamy,
- zapchana skrzynka,
- nie kończące się listy RBL z naszą domeną pocztową,
- częste braki w dostępie,
- słaba wydajność połączenia pomiędzy klientem poczty elektronicznej a serwerem pocztowym,
- problemy z wysyłkami maili do niektórych odbiorców, brak wspólnej bazy adresowej itp.
- i wiele osób pozdrawiających nas od ***Mój przyjacielu*** (i to kilka razy dziennie), chociaż nigdy o nadawcy nie słyszeliśmy…

Konsekwencje używania tanich lub bezpłatnych skrzynek pocztowych są najczęściej przykre i trudne do usunięcia. Można tego wszystkiego uniknąć, korzystając z profesjonalnej skrzynki pocztowej w ramach subskrypcji produktu Office 365 Business Essentials.

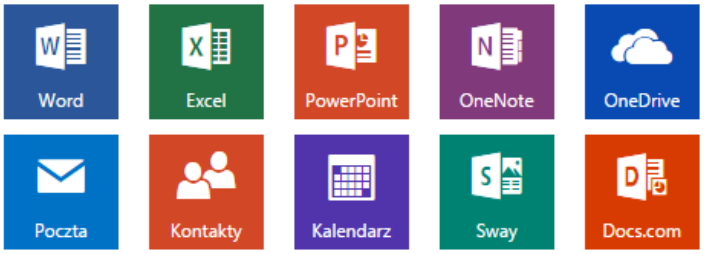
Czy wiesz, że :

- **87% wirusów i innego kodu niepożądanego, dostaje się do środowiska ofiary poprzez wiadomość e-mail**
- **63% firm odnotowało od 2 do 5 różnych ataków w ciągu ostatniego roku**

Dlatego proponujemy jedną z najlepszych skrzynek mailowych klasy biznesowej –

Office 365
Business Essentials

Microsoft



Co to jest Office 365 BE :

- **poczta e-mail i kalendarze** : poczta e-mail klasy biznesowej w rozbudowanym i znajomym interfejsie programu Outlook — możesz do niego uzyskiwać dostęp z komputera stacjonarnego lub przeglądarki internetowej przy użyciu aplikacji Outlook Web App. Skrzynki pocztowe są rozmiarze 50 GB na użytkownika z możliwością wysyłania załączników o wielkości do 150 MB
- **przechowywanie i udostępnianie plików** : usługa OneDrive dla Firm udostępnia 1 TB przestrzeni dyskowej dla każdego użytkownika i umożliwia dostęp do dokumentów niemal z dowolnego miejsca. Udostępniaj pliki innym osobom z Twojej organizacji i spoza niej, kontroluj, kto może wyświetlać i edytować poszczególne pliki, oraz łatwo synchronizuj pliki z komputerami PC i Mac i innymi urządzeniami
- **konferencje online** : możliwość organizacji spotkań online z zawartością audio i wideo, korzystając z udostępniania ekranu i konferencji wideo w jakości HD dostępnych po jednym kliknięciu
- **wiadomości błyskawiczne i łączność programem Skype** : kontaktuj się z innymi użytkownikami programu Skype dla firm za pomocą wiadomości błyskawicznych, połączeń głosowych i wideo, a także informuj o swojej dostępności za pomocą statusu. Przekazuj użytkownikom programu Skype informacje o obecności, wysyłaj im wiadomości błyskawiczne i korzystaj z połączeń audio
- **firmowa sieć społecznościowa** : media społecznościowe mogą również występować wewnątrz firmy – nie tylko w sieci Internet. Oprogramowanie do współpracy i aplikacje biznesowe Yammer umożliwiają pracownikom nawiązywanie połączeń z odpowiednimi osobami,

udostępnianie informacji w zespołach i organizowanie projektów tak, aby można je było szybciej realizować

- **witryna zespołów** : podstawowy magazyn 1 TB oraz 500 MB miejsca do magazynowania dla każdego użytkownika zapewniają łatwy dostęp do dokumentów oraz możliwość ich udostępniania
- **pakiet Office Online** : tworzenie i edytowanie dokumenty programów Word, OneNote, PowerPoint i Excel w przeglądarce
- **zarządzanie pracą** : usługa Planner ułatwia Twojemu zespołowi tworzenie nowych planów, organizowanie i przypisywanie zadań, udostępnianie plików, prowadzenie rozmów o wykonywanych czynnościach oraz informowanie o postępach w pracy – oszczędność czasu
- **wyszukiwanie i odnajdywanie** : bądź na bieżąco. Wyszukuj i odnajduj zawartość w usłudze Office 365 na podstawie spersonalizowanych analiz. Aplikacja Office Delve to pierwsze rozwiązanie, które korzysta z funkcji Office Graph, kolekcji przeanalizowanych sygnałów lub wniosków wyciągniętych na podstawie zachowania poszczególnych użytkowników i ich relacji z zawartością, tematami i kontaktami
- **niezawodność** : możesz spać spokojnie - Twoje usługi są dostępne przez 99,9% czasu (gwarantowane) na podstawie umowy SLA
- **zabezpieczenia** : nowatorskie metody zapewniania bezpieczeństwa z pięcioma warstwami zabezpieczeń i proaktywnym monitorowaniem zapewniają ochronę danych wszystkich użytkowników zasobów firmowych
- **ochrona prywatności** : Twoje dane należą do Ciebie. Chronimy je i zapewniamy poufność informacji
- **administracja** : wdrażanie usługi Office 365 BE w Twojej firmie i zarządzanie nią, nie wymagają specjalistycznej wiedzy informatycznej. Możesz dodawać i usuwać użytkowników w ciągu kilku minut.
- **najnowsza wersja** : nie ma opłat za uaktualnienia wersji — aktualizacje są uwzględnione w subskrypcji. Nowe funkcje są regularnie przekazywane klientom usługi Office 365

Połączenie jednego z najlepszych rozwiązań do ochrony sieci lokalnej UTM firmy Fortinet z najlepszą, biznesową skrzynką pocztową na tej planecie, powoduje, że otrzymujemy najlepszą ochronę naszych danych cyfrowych, tożsamości, prywatności, spokojnego działania firmy w niemal każdych warunkach.

Fortinet UTM

+

Office 365 Business Essentials

=

Bezpieczeństwo

[im taniej, tym gorzej]

Przy opracowaniu przewodnika, korzystaliśmy z materiałów firm Fortinet i Microsoft oraz z **własnego wieloletniego doświadczenia** w korzystaniu wymienianych tu technologii i rozwiązań, z których korzystamy na co dzień i nie wyobrażamy sobie pracy inaczej, jak przy ich udziale.

Gorąco zachęcamy do odwiedzenia naszej strony poświęconej poruszanym zagadnieniom, a także do kontaktu z nami – jesteśmy otwarci na każdy problem. Każdy z nich można rozwiązać, a efekty będą z pewnością wymierne.

Celowo w naszym przewodniku, nie poruszaliśmy kwestii jak wycenić koszt poniesionych strat, w wyniku działania kodu niepożądanego, ponieważ są one w dużej mierze nie mierzalne i mocno subiektywne, niemniej jednego jesteśmy pewni - nakłady na bezpieczeństwo sieci, komputerów i użytkowników, są ułamkiem tego, ile firma straci w danych.

Przykład – za utratę plików JPK (szczególnie tych już podpisanych i wysłanych), które należy chronić w najwyższym możliwym stopniu (zawierają przecież wszystkie dane finansowe każdej firmy), będzie groziła bardzo wysoka kara, nie licząc strat wizerunkowych, odtworzeniowych oraz tej najważniejszej – kto zapoznaje się z moimi danymi finansowymi, jeśli są one w posiadaniu osób nieupoważnionych ?
Czy warto ryzykować ?

Bezpieczeństwo jest podstawą – nie znosi kompromisów.

Zespół KOMAKO.asp


http://www.
Favorites