Obrona cyberprzestrzeni

Cyberbezpieczeństwo jest integralną częścią każdej koncepcji bezpieczeństwa korporacyjnego lub krajowego

Wprowadzenie

Zagrożenia dla danych pochodzą ze wszystkich azymutów. Dane są zagrożone zarówno podczas przechowywania, jak i podczas transportu, a specjaliści ds. Bezpieczeństwa danych muszą wdrożyć czujniki i bariery, aby żadne złośliwe oprogramowanie nie mogło wpłynąć na dane organizacji. Istnieje mnóstwo technik i narzędzi, które chronią dane, a przy odpowiednim wdrożeniu maksymalizują bezpieczeństwo systemu informatycznego. Narzędzia bezpieczeństwa danych można ogólnie pogrupować w zorientowane na ochronę komputera i ochronę sieci, przy czym te pierwsze dotyczą danych tworzonych lub przechowywanych na komputerze, a te drugie dotyczą danych w tranzycie podróżujących przez sieci.

Aplikacje do ochrony plików

Istnieje wiele pojedynczych funkcji, a także kompleksowe oprogramowanie do ochrony plików, które po zainstalowaniu chronią komputer przed wieloma niepożądanymi zdarzeniami.

Kopia zapasowa pliku

Tworzenie kopii zapasowych plików jest podstawową funkcją, którą musi mieć każda stacja robocza lub system informacyjny. Kopia zapasowa plików może odbywać się w trybie offline na podłączonym urządzeniu wymiennym lub w systemie pamięci masowej dostępnym w intranecie lub online przez FTP w lokalizacji dostępnej w Internecie. Przechowywanie kopii zapasowych może odbywać się w czasie rzeczywistym, zgodnie z harmonogramem lub na żądanie. Pamięć może mieć opcje szyfrowania i kompresji. Ponadto opcje przechowywania kopii zapasowych często oferują „automatyczną archiwizację starych wersji". Chociaż nie jest to zalecane, większość aplikacji do tworzenia kopii zapasowych oferuje partycjonowanie głównego dysku, tworząc obszar kopii zapasowych plików. Chociaż jest to lepsze niż brak tworzenia kopii zapasowej, najlepiej miejsce na kopię zapasową musi znajdować się na fizycznie innym nośniku. Rysunek 8.1 ilustruje różne opcje tworzenia kopii zapasowych plików. Chociaż tworzenie kopii zapasowych plików jest niewątpliwie koniecznym środkiem, odzyskiwanie może być bardzo czasochłonnym procesem ponownej instalacji setek aplikacji i plików. Można tego uniknąć, jeśli zamiast tworzyć kopię zapasową plików, od czasu do czasu wykonywana jest kopia zapasowa pełnego obrazu zagrożonych dysków. Ten obraz binarny, archiwizowany z częstotliwością ustalaną przez administratora danych, będzie znacznie szybciej mapowany z powrotem na dyski w celu szybkiego i bardziej wiernego odzyskiwania. Obraz nośnika pamięci jest pojedynczym plikiem binarnym, który zawiera każdy bit tego nośnika, w tym wszystkie bity partycjonowania sektora. Takim nośnikiem może być taśma, dysk USB lub dowolny dysk (twardy, dyskietka, CD, DVD itp.), Gdzie obraz jest idealną logiczną repliką zarchiwizowanego nośnika.

Odzyskiwanie po awarii

Odzyskiwanie po awarii dotyczy sytuacji awaryjnych, w których pliki operacyjne organizacji są uszkodzone w stopniu przekraczającym dopuszczalne użycie. Odzyskiwanie po awarii wymaga, aby całe oprogramowanie organizacji było przechowywane w co najmniej dwóch lokalizacjach, jednym w siedzibie, a drugim poza lokalem, i było dostępne online. Systemy odzyskiwania po awarii składają się z serwerów i dużych urządzeń pamięci masowej zapewniających szeroki zakres funkcji, w tym:

• Kopia zapasowa obrazu dysku

• Kopia zapasowa plików operacyjnych i archiwalnych

• Kopia zapasowa aplikacji (z przechowywaniem numerów licencji)

• Przywracanie systemu od zera (mapowanie binarne)

• Tworzenie kopii zapasowej na dysku / udziale sieciowym

• Tworzenie kopii zapasowych na taśmach i bibliotekach taśm

• Tworzenie kopii zapasowych w pamięci online

• Zdalne i scentralizowane zarządzanie

• Katalog kopii zapasowych i wyszukiwanie

• Przywróć na innym sprzęcie lub maszynie wirtualnej (VM)

• Usuwanie duplikatów

Termin „duplikacja" oznacza usunięcie wszystkich duplikatów, więc cokolwiek jest przechowywane lub przesyłane, jest tak unikalne, jak to możliwe. W ten sposób wymagana pojemność pamięci i czas transmisji po awarii są zminimalizowane. Odzyskiwanie po awarii, które jest bardzo podstawową funkcją organizacji, wymaga przydzielenia dedykowanego zespołu do tego zadania, który dzięki szkoleniom i praktyce może zapewnić ciągłość biznesową w minimalnym czasie.

Usuwanie historii

Usuwanie historii może być bardzo ważną kwestią w wielu organizacjach. W starym papierowym świecie niszczarka papieru lub pojemnik na ogień całkowicie wyeliminowałyby istnienie wybranych dokumentów. Chociaż istnieje wiele elektronicznych sposobów niszczenia dokumentu elektronicznego, agencje wywiadowcze często wymagają, aby fizyczny nośnik, na którym rezyduje lub znajduje się wrażliwy dokument elektroniczny, był fizycznie niszczony na małe kawałki o wymiarach mniejszych niż 4 × 4 mm. Komunikat, wynikający z tej opcji, jest taki, że żadne elektroniczne usuwanie plików nie jest wystarczająco silne, aby absolutnie zaufać. Wiele przeglądarek internetowych oferuje prywatne tryby surfowania, zwane incognito, inPrivate lub innymi nazwami, w których twierdzi się, że po wyjściu z tego trybu komputer nie zachowuje śladu surfowania w tym trybie. Według ekspertów kryminalistyki dostępne są narzędzia umożliwiające odzyskiwanie takich plików i innych danych.

Niszczenie i wycieranie

Niszczenie plików jest procesem elektronicznym, w którym plik jest kilkakrotnie zapisywany z kilkoma wzorami, tak więc według twórcy e-shreddera plik jest całkowicie niszczony. Wiele produktów antywirusowych zawiera niszczarkę elektroniczną. Wymazywanie dysku to koncepcja całkowitego wyczyszczenia dysku i sformatowania go. Jest to potrzebne w przypadku przenośnych urządzeń pamięci masowej, dysków twardych lub półprzewodnikowych urządzeń USB. Takie produkty „całkowicie i łatwo usuwają wszystkie dane na żywo, aby nie można było ich odzyskać za pomocą żadnej istniejącej technologii".

Odzyskaj plik

Cofnięcie usunięcia pliku pozwala odzyskać określony plik, który został usunięty. Po usunięciu pliku jego zawartość nie jest usuwana, tylko jego miejsce jest dodawane na liście dostępnych sektorów. Z tego powodu usunięty plik może zostać przywrócony, chyba że został faktycznie nadpisany. Dostępnych jest kilka skutecznych narzędzi z wystarczającą liczbą parametrów wyszukiwania, co

pozwala wykryć pliki i cofnąć proces usuwania krócej niż w innych przypadkach, choć czasami mierzone w godzinach

Szyfrowanie plików

Szyfrowanie plików jest niezbędną praktyką w utrzymywaniu bezpieczeństwa plików, ale posiadanie hasła do każdego dokumentu może przynieść efekt przeciwny do zamierzonego.

Jednak poufne dokumenty wymagają ochrony i należy zidentyfikować opcję szyfrowania. Pakiety automatyzacji pakietu Office zapewniają opcję szyfrowania, w której w razie potrzeby można przypisać dwa hasła, jedno tylko do odczytu, a drugie do modyfikacji. Można używać zewnętrznych aplikacji szyfrujących, które zapewniają równie silne szyfrowanie. Inne oprogramowanie do szyfrowania umożliwia tworzenie „wirtualnego zaszyfrowanego dysku w pliku ... [który można zamontować] ... jako dysku wirtualnego, do którego można uzyskać dostęp za pomocą litery dysku" .Może to być dysk główny lub przenośny. Gdy pliki są przechowywane na tym dysku wirtualnym, są one szyfrowane i przenoszą klucz hasła dysku. Jest to bardzo interesująca technologia, w której nie ma potrzeby stosowania indywidualnych haseł dla poszczególnych plików.

Rejestratory

Rejestratory to oprogramowanie lub sprzęt, które kopiują informacje podczas ich generowania i przechowują je w określonym miejscu. To miejsce może znajdować się na komputerze, na którym informacje zostały wygenerowane, lub może być w odległym miejscu dostępnym w sieci, przewodowym lub bezprzewodowym. Administrator może zainstalować rejestrator w celu gromadzenia statystyk do analizy lub w celu tajnego monitorowania niczego niepodejrzewającego użytkownika. Możliwe jest również, że haker sieciowy zainstaluje program rejestrujący na niechronionym komputerze. Zarejestrowane informacje mogą być przechowywane lokalnie lub zdalnie. W tym drugim przypadku komunikacja może odbywać się za pośrednictwem

• FTP, wysłane na serwer lub bazę danych

• E-mail w regularnych odstępach czasu

• Bezprzewodowy oznacza — Wi-Fi lub Bluetooth

• Zdalne logowanie - komunikacja między komputerami

Klawiatura jest głównym interfejsem człowiek-maszyna i jest bardzo wrażliwym punktem wejścia. Rejestratory klawiszy działają w różnych trybach, przy czym najłatwiej jest to zrobić dzięki oprogramowaniu zainstalowanemu w tym celu. Inne tryby to fale akustyczne lub elektromagnetyczne. Wciśnięcie każdego klawisza generuje niepowtarzalny dźwięk oparty na mechanicznej konstrukcji klawiatury, i możliwe jest, że dźwięki te zostaną zarejestrowane i przeanalizowane, co prowadzi do sekwencji naciśnięć klawiszy. W przypadku klawiatur bezprzewodowych komunikacja może być przechwytywana z powietrza i podobnie ujawnia naciśnięcia klawiszy. W klawiaturach przewodowych przewody łączące promieniują fale elektromagnetyczne, reprezentując standardowe sekwencje zer i jedynek odpowiadające naciśnięciom klawiszy.

Anti-Loggery

Anty-loggery to oprogramowanie zaprojektowane specjalnie do wykrywania obecności kodu rejestrującego. Chociaż typowe oprogramowanie antywirusowe wykrywa wiele trybów rejestrowania, dedykowane oprogramowanie antywirusowe może lepiej to obsłużyć i bardzo ważna potrzeba bezpieczeństwa. Za pierwszym razem szyfrowanie naciśnięć klawiszy zostało aktywowane, co

spowodowało, że pismo zostało wyróżnione pogrubioną czcionką. Po raz drugi słowo zostało wpisane po dezaktywacji szyfrowania klawiszy. Podczas aktywacji keyloggera, zainstalowane oprogramowanie antywirusowe zostało ostrzeżone, że ten program może być niebezpieczny.

Aplikacje wydajności komputera

Aby komputer działał w najlepszym wydaniu, pliki i ich wzajemne relacje muszą być wolne od błędów. Dostępne są aplikacje, które skanują komputer, identyfikują błędy i przywracają pliki do prawidłowego stanu. Takie aplikacje obejmują następujące funkcje, które mają zapewnić stabilną pracę komputera i maksymalną dostępność zasobów.

• Naprawa rejestru

• Anti-rootkity

• Antywirus

• Niepotrzebne pliki

• Fragmentacja

Naprawa rejestru

W systemie operacyjnym rejestr plików - centralna baza danych systemu - ułatwia komunikację między plikami i dostęp do plików. Z czasem jednak gromadzą się stare i luźne pliki, które często są uszkodzone. Gdy wystąpią błędy rejestru, komputer zwalnia, aplikacje się zawieszają, a sam komputer często ulega awarii. „Naprawiając te przestarzałe informacje w rejestrze systemu Windows, system będzie działał szybciej i bezbłędnie” [14]. Tabela 8.4 zawiera listę typowych błędów wykrytych i naprawionych przez narzędzia do naprawy rejestru.

Anti-Rootkity

Rootkit to złośliwe oprogramowanie szpiegujące, które hakerzy wkładają do aplikacji lub systemu operacyjnego w celu utworzenia zapadni. Dostęp do zapadni omija wszystkie kontrole bezpieczeństwa. Dzięki tym zapadniom hakerzy omijają wszystkie środki bezpieczeństwa i uzyskują dostęp do zasobów jako autoryzowany użytkownik. „Rootkity mogą leżeć ukryte na komputerach i pozostać niewykryte przez oprogramowanie antywirusowe”. Anti-rootkity sprawdzają każdą nową instalację programu w poszukiwaniu programów szpiegujących. Usunięcie oprogramowania szpiegującego z aplikacji jest jak operacja chirurgiczna i musi zostać wykonane bez wpływu na nominalną wydajność aplikacji. Rootkity w programach zainstalowanych przed instalacją rootkita mogą nie zostać wykryte. Dlatego zaleca się ponowną instalację programów po instalacji programu antywirusowego.

Antywirusowe

Wirus to złośliwe oprogramowanie, które uszkadza pliki, powoduje problemy operacyjne i powoduje awarie aplikacji, a często także systemu operacyjnego. Najczęstszym działaniem wirusa jest pisanie na obszarach przeznaczonych dla systemu operacyjnego i sterowników lub na kodzie aplikacji.

Niepotrzebne pliki

Niepotrzebne pliki to pliki, które zostały odinstalowane przez procesy lub nie są już powiązane z żadną prawidłową aplikacją. Rezultatem jest szybszy wykonywanie aplikacji, usuwane byłyby niepotrzebne programy do czyszczenia plików

• Pliki tymczasowe systemu Windows

• Nieprawidłowe menu startowe

• Przestarzałe pliki w plikach programu

• Nieprawidłowe skróty

• Nieprawidłowe pliki msi

• Zdefiniowane przez użytkownika niepotrzebne pliki i foldery

• Puste pliki i foldery

• Nieprawidłowe pliki i foldery

Fragentacja

Termin fragmentacja odnosi się do sposobu zapełniania dysku twardego. Ponieważ miejsce na dysku twardym jest wykorzystywane do operacji ciągłego zapisu i usuwania, tworzone są puste przestrzenie zwane fragmentami. Fragmenty zapobiegają ładowaniu dużych aplikacji w sąsiadujących sektorach. Aplikacje przechowywane w różnych nieciągłych sektorach na dysku twardym wymagają użycia do zarządzania pamięcią, co spowalnia działanie konkretnej aplikacji. Defragmentacja próbuje skonsolidować całą dostępną przestrzeń razem, aby duże aplikacje mogły być instalowane bez partycji. Problemy spowodowane fragmentacją plików obejmują

• Awarie i system zawiesza się / zawiesza

• Powolne uruchamianie i komputery, które nie uruchamiają się

• Długi czas tworzenia kopii zapasowej i przerwana kopia zapasowa

• Uszkodzenie pliku i utrata danych

• Błędy w programach

• Wykorzystanie pamięci RAM i problemy z pamięcią podręczną

• Awarie dysku twardego

• Ogólna powolna wydajność serwera domino

• Długotrwałe blokady w dzienniku konsoli

• Limity czasu semaforów

Narzędzia ochronne

W wyniku bycia częścią cyberprzestrzeni system informacyjny jest narażony na wiele niebezpieczeństw. Na szczęście istnieje również wiele aplikacji cyberobrony, które minimalizują to ryzyko. Trochę aplikacje, które są łatwo dostępne, opisano poniżej.

Analizator bezpieczeństwa

Istnieje bardzo przydatne narzędzie oferowane bezpłatnie, które zapewnia dogłębną analizę cyberbezpieczeństwa hosta podłączonego do sieci. Jest to Microsoft Baseline Security Analyzer (MBSA). To narzędzie skanuje komputer i dla każdego wykrytego problemu generuje raport z analizy bezpieczeństwa

• Co zostało zeskanowane

• Szczegóły wyniku

• Jak to naprawić

MBSA może przeskanować pojedynczy komputer lub wiele komputerów lub może pobrać raporty ze skanowania z wcześniejszych analiz. MBSA to narzędzie systemu Windows, sprawdzające i raportujące następujące kwestie:

• Luki administracyjne w systemie Windows

• Luki administracyjne IIS (Internet Information Services)

• Luki administracyjne w SQL

• Aktualizacje bezpieczeństwa

Problemy sprawdzone przez MBSA obejmują

• Lokalne hasła dostępu

• Obecność

• Wygaśnięcie

• Siła

• Konfiguracja systemu plików

• uprawnienia administracyjne

• Konta gości

• Niekompletne aktualizacje

• Zapora systemu Windows

• Audyt zdarzeń - logowanie / wylogowywanie

• Zainstalowane usługi

• Wspólne zasoby - dyski

Raport przedstawia zidentyfikowane problemy i zawiera kroki dla rozwiązania każdego problemu. Jest to bardzo proste narzędzie, które musi być zainstalowane na każdym komputerze i często uruchamiane.

Analizator haseł

Istnieje wiele metod i oprogramowania do łamania haseł oraz znajomość „siły" używanych przez nas haseł może być bardzo ważna. Wiele systemów informatycznych automatycznie odrzuca przypisywanie „słabych" haseł. Istnieje wiele teorii na temat tego, co stanowi silne lub słabe hasło, i istnieje wiele mierników haseł w Internecie. Hasła takie jak hasło uzyskują wynik 8%, a hasło takie jak Uo5 $ Pw9 # 3 otrzymuje wynik 100%.

Hasła w systemach operacyjnych Windows są przechowywane w znanych lokalizacjach, ale w formie skrótowej. To znaczy hasło to przetaczane przez algorytm mieszający i generowany jest kod. Jednak znanych jest wiele algorytmów mieszających. Dlatego jeśli hasło hashcode odpowiada hashcode znanego hasła, można stwierdzić, że znaleziono nieznane hasło. Wśród aplikacji do wykrywania haseł

znajduje się oprogramowanie Cain & Abel Password Protection (C&A) , które zostało zaprojektowane dla systemów operacyjnych Microsoft i twierdzi, że wykonuje następujące czynności:

• Umożliwia łatwe odzyskanie kilku rodzajów haseł poprzez wąchanie sieci

• Łamanie zaszyfrowanych haseł za pomocą

• Atak słownikowy

• Brutalny atak

• Atak kryptoanalizy

• Nagrywanie rozmów VoIP

• Dekodowanie zaszyfrowanych haseł

• Odzyskiwanie kluczy sieci bezprzewodowej

• Ujawnianie skrzynek z hasłami

• Odkrywanie buforowanych haseł

• Analiza protokołów routingu

W technice Ataku Słownikowego obliczane są kody skrótu odpowiadające rzeczywistym słowom. Każdy hashcode jest porównywany z hashcode hasła. W przypadku dopasowania zakłada się, że słowo odpowiadające pasującemu hashcode jest poszukiwanym hasłem. Zaletą tej metody jest to, że jest ona dość szybka i prosta. Jeśli jednak hasło nie jest prawidłowym słowem, ale zawiera znaki specjalne lub cyfry, technika ta zawodzi.

W technice Ataku Brute Force generowane są skróty wszystkich możliwych kombinacji znaków, a ostatecznie znajduje się hasło. Proces ten może potrwać długo, w zależności od dostępnej mocy obliczeniowej, ale teoretycznie na końcu znajduje się hasło. W technice ataku kryptoanalizacyjnego w bazach danych dostępne są wstępnie obliczone kody skrótu odpowiadające rzeczywistym hasłom alfanumerycznym, zwane tablicami Rainbow. Hashcode hasła pobrany z listy komputerów PC jest porównywany z hashcodes w bazie danych, w której można znaleźć dopasowanie, w zależności od wielkości bazy danych. Dodatkowe usługi świadczone przez C&A obejmują:

Sniffer analizujący zaszyfrowane protokoły i analizujący sieć i ruch

Przeglądarka haseł, która może ujawniać hasła aplikacji Microsoft

Dumper, która zrzuca Tajemnice lokalnego organu bezpieczeństwa (LSA)

Dekoder haseł, który może ujawniać hasła połączeń telefonicznych przechowywane w systemie Windows

Bezprzewodowy skaner, który zbiera parametry identyfikacji i wydajności w dostępnych urządzeniach Wi-Fi, a także może przechwytywać i dekodować zaszyfrowane pliki 802.11

Skaner SID, który uzyskuje dostęp do zdalnego systemu i wydobywa zabezpieczenia identyfikatora

Filtr VoIP, który rejestruje rozmowy VoIP w formacie WAV

LAN Scanner, który rozpoznaje obecność snifferów sieciowych i systemów wykrywania włamań

Zapory ogniowe

Zapora to kontroler ruchu dla ruchu przychodzącego, wychodzącego lub dwukierunkowego. Oczekiwane korzyści z zapory ogniowej powinny obejmować

• Kontrolowany dostęp do zasobów korporacyjnych

• Zapobieganie nieautoryzowanemu dostępowi do aplikacji lub informacji

• Integracja z mechanizmami uwierzytelniania użytkowników

• Bezpieczne wdrażanie nowych aplikacji

• Ochrona firmowych adresów sieciowych przed Internetem

• Bezpieczny zdalny dostęp do sieci korporacyjnej

• Wykrywanie i zapobieganie włamaniom w całym przedsiębiorstwie

• Mechanizm filtrowania treści

Może to być wyłącznie oprogramowanie lub oprogramowanie zainstalowane na dedykowanym sprzęcie.

W stosie hierarchicznym zapora zwykle znajduje się w warstwie sieci, ale można ją również znaleźć w warstwie transportowej.

Filtrowanie na poziomie pakietów

Ponieważ wszystko w nowoczesnej sieci przenosi się w pakietach danych, filtrowanie odbywa się na poziomie pakietu. Pakiety zawierają liczby binarne lub kody, które zawierają następujące informacje:

• Pochodzenie pakietu - adres IP i numer portu

• Miejsce docelowe pakietu - adres IP i numer portu

• Informacje o protokole

• Znak czasu

• Ładunek - dane, polecenia lub potwierdzenie

• Informacje o wykrywaniu błędów

• Inne - serializacja danych, priorytet itp.

W filtrowaniu na poziomie pakietów, które jest instalowane w warstwie sieciowej, zapory ogniowe odbierają pakiety i oceniają ich potencjalne zagrożenie. Ocena oparta na powyższych trzech pierwszych parametrach (źródle, miejscu docelowym i protokole) zwykle kończy się jedną z dwóch poniższych opcji:

• Pakiety są przekazywane do miejsca docelowego.

• Pakiety są opóźniane, jeśli podejrzewa się atak DoS.

• Pakiety są odrzucane.

Jest to bardzo proste podejście do ochrony, ale można go oszukać za pomocą pakietów o sfałszowanych adresach. Termin sfałszowany odnosi się do fałszowania parametrów pakietu, głównie adresu IP.

Filtrowanie na poziomie obwodu

Ta kategoria zapór ogniowych jest zwykle instalowana w warstwie transportowej, gdzie weryfikuje sesję przed wydaniem oceny wiarygodności pakietów. Kryteriami są powyższe cztery pierwsze parametry (pochodzenie, miejsce docelowe, protokół i znacznik czasu), a także poświadczenia użytkownika - nazwa użytkownika i hasło. Przy takich kryteriach fałszowanie adresów IP nie jest jedynym decydującym czynnikiem w ocenie pakietu.

Brama na poziomie aplikacji

W tym przypadku zapora ogniowa to inteligentny serwer proxy chroniący host przed siecią. Zapora ogniowa dokonuje wymiany danych w sposób przezroczysty dla zdalnego systemu i może kontrolować przepływ pakietów w oparciu o wyrafinowane kryteria ustalone przez administratora sieci. Ten typ zapory często ma możliwość szyfrowania i deszyfrowania danych, co zwiększa bezpieczeństwo. Brama na poziomie aplikacji jest zdecydowanie najbezpieczniejszą zaporą ogniową, ale jednocześnie najbardziej złożoną, wymagającą własnego sprzętu.

Ochrona poczty e-mail

E-mail można chronić na trzy sposoby. Jednym z nich jest potężny klient poczty e-mail, który zapewnia szeroką ochronę, gdy wiadomości przychodzą do przeglądania.

Innym jest oprogramowanie zainstalowane na tym samym hoście z klientem e-mail i praca z klientem e-mail. Trzecie podejście to outsourcing, w którym system poczty elektronicznej organizacji jest rezydentem i jest zarządzany w chmurze. Chmura to termin opisujący korzystanie z Internetu , usługi zlecone na zewnątrz i znajdujące się poza siecią fizyczną organizacji. W chmurze „jest hostowany poza… [siecią organizacji]… sieci, nie wymagając dodatkowego sprzętu, oprogramowania ani zasobów ludzkich do zarządzania codziennymi operacjami bezpieczeństwa". Postępy w technologiach szkodliwego oprogramowania wymagają bezpiecznych systemów pocztowych gdzie oczekiwane funkcje i korzyści obejmują:

• Filtrowanie poczty przychodzącej

• Filtrowanie wiadomości wychodzących

• Filtrowanie antyspamowe w wielu językach

• Blokowanie złośliwego oprogramowania

• Kwarantanna spamu

• Kontrola załączników antimalware

• Usunięcie regulowanych treści

• Szyfrowanie i deszyfrowanie w celu przechowywania lub transportu

• Egzekwowanie zasad korporacyjnych

• Odzyskiwanie po awarii

• Archiwizacja wiadomości e-mail

Zaawansowane systemy filtrowania powiadamiają o rozpoznawaniu obrazów, jeśli treść wiadomości e-mail lub załączniki zawierają obrazy z podpisami cyfrowymi, które spełniają określone cechy. Dodatkowe korzyści zapewniane przez oparty na chmurze system poczty elektronicznej obejmują

• Brak sprzętu lub oprogramowania do zainstalowania lub zarządzania

• Brak nakładów kapitałowych z góry, kosztów instalacji i aktualizacji

• Obsługa klienta 24 × 7

• Automatyczne włączanie i synchronizacja w celu zapewnienia ciągłości

• Zintegrowana internetowa konsola administracyjna dla wszystkich rozwiązań

• Powiadomienia o naruszeniach zasad, zablokowanych treściach i poddanych kwarantannie wiadomości

• Ochrona przed atakami

Typowe ataki na systemy pocztowe obejmują DoS i próby kopiowania katalogów.