Wstęp

Abstrakt

Poczta elektroniczna jest obecnie dla wszelkiego rodzaju firm i organizacji niekomercyjnych najistotniejszym medium komunikacji – zarówno wewnętrznej jak i zewnętrznej. Mimo rozpowszechnienia się różnego rodzaju branżowych i uniwersalnych portali służących do wymiany informacji, systemów obiegu dokumentów funkcjonujących wewnątrz struktury organizacyjnej oraz innych systemów komunikacji elektronicznej, e-mail pozostaje podstawowym środkiem wymiany informacji z pracownikami, klientami i partnerami. Dlatego też kwestia bezpieczeństwa systemów e-mail nabiera pierwszorzędnego znaczenia. Wbrew pozorom pojęcie bezpieczeństwa poczty elektronicznej to dużo wiecej niż walka ze spamem i wirusami – i właśnie o wszystkich tych zagadnieniach traktuje niniejsza książka.

Systemy filtrowania poczty elektronicznej nabierają coraz większego znaczenia we współczesnych przedsiębiorstwach. Tradycyjna rola tego typu systemu ograniczała się jeszcze parę lat temu do wykrywania wirusów oraz do działań antyspamowych. Obecnie wraz ze stałym wzrostem znaczenia komunikacji elektronicznej zakres działania filtrów e-mail znacząco się poszerzył – stały się one jednym z kluczowych ogniw systemów DLP (*Digital Leak Pevention*) – tj. systemów zapobiegania wyciekom danych z systemów komputerowych. Rola antyspamowa i antywirusowa bramek e-mail jest oczywiście dalej bardzo istotna, jednak nie mniej ważna staje się realizacja takich zadań jak np.: skanowanie słownikowe, wykrywanie typów załączników na podstawie sygnatur binarnych czy wykrywanie fragmentów(!) poufnych dokumentów na podstawie wcześniej zadanych wzorców. Jak wykazują badania, tradycyjny e-mail obok systemów webmail oraz różnego rodzaju portali webowych jest głównym źródłem wycieku poufnych informacji z firmy. Wyciek cennych danych nie musi być zawsze spowodowany świadomym i złośliwym działaniem (tj. klasycznym szpiegostwem przemysłowym). Praktyka wykazuje, że typowo dane tracone są nie z powodu złej woli, lecz raczej z powodu nieuwagi, braku odpowiedniego przeszkolenia oraz niefrasobliwości pracowników. Niezależnie jednak od przyczyny skutki takich zdarzeń bywają dla firm katastrofalne, zarówno w sensie bardzo wymiernym (np. w przypadku ujawnienia listy płac lub wyników finansowych), jak i w sensie wpływu na wizerunek firmy (np. gdy ujawniona zostanie „prywatna" korespondencja wyższego kierownictwa). Kompleksowe bezpieczeństwo systemu e-mail wymaga więc kontroli poczty wchodzącej i poczty wychodzącej. O ile w pierwszym przypadku dbamy przede wszystkim o szeroko pojęta „higienę" wewnętrznych zasobów firmy, o tyle w przypadku poczty wychodzącej staramy się zapobiec sytuacjom mogącym zagrozić reputacji firmy, prowadzonemu przez nią biznesowi, a w najbardziej drastycznych przypadkach nawet jej istnieniu.

W niniejszej książce sklasyfikowano i opisano zagrożenia, jakie niesie ze sobą stosowanie poczty elektronicznej; następnie przedstawiono metody ograniczenia tych zagrożeń. Omówiono też architekturę systemów filtracji poczty oraz przykłady dostępnych systemów, zarówno darmowych, jak i komercyjnych. Dla Czytelników

niezaznajomionych z tematyką funkcjonowania systemów poczty elektronicznej przedstawiono charakterystykę protokołu SMTP oraz zasady konstrukcji wiadomości e-mail – w tym standard MIME pozwalający na obsługę załączników.

Książka jest przeznaczona dla administratorów systemów e-mail, osób odpowiedzialnych za bezpieczeństwo informatyczne, kierowników działów IT, studentów kierunków informatycznych oraz wszystkich zainteresowanych tematyką bezpieczeństwa systemów IT.

Od Czytelnika oczekuje się znajomości podstaw funkcjonowania sieci komputerowych i systemów operacyjnych.

Wszystkich Czytelników, którzy chcieliby podzielić się ze mną uwagami na temat książki, zachęcam do kontaktu mailowego: *g.blinowski@ii.pw.edu.pl*.

Grzegorz Blinowski

Podziękowania

Pragnę podziekować sponsorom: Instytutowi Informatyki Politechniki Warszawskiej oraz firmie McAfee Polska – bez nich wydanie tej książki nie byłoby możliwe. Dziękuję także mojej Żonie za wnikliwą korektę.