CRN Vademecum
01.09.14 nr: - str. 1 nakład: 6000 egz.

Ochrona sieci
Wyzwanie dla integratorów
str. 12

CRN Vademecum
01.09.14 nr: - str. 1 nakład: 6000 egz.

Coraz większe wyzwanie

Wielu przedsiębiorców do ochrony swoich sieci wykorzystuje rozwiązania starszego typu. Tymczasem tradycyjne firewalle i hasła przestały odpowiadać naturze dzisiejszych ataków i nie stanowią już skutecznych „zasieków" na informatycznej granicy firmy.

TOMASZ JANOŚ

Ukierunkowane ataki APT, DDoS złośliwe oprogramowanie ransomware (używane do wymuszania okupu), coraz bardziej wymyślne formy w komunikacji botnetów... Wszystko to wymaga nowego spojrzenia na dotychczasowe metody zabezpieczenia systemów informatycznych. Dodatkowo producenci rozwiązań zabezpieczających muszą podążać za takimi trendami rynkowymi, jak: konsumeryzacja IT, praca ma odległość, powszechna wirtualizacja systemów oraz przetwarzanie danych w chmurze. Nic dziwnego, że od kilku lat zarówno dostawcy rozwiązań, jak i konsultanci do spraw bezpieczeństwa promują trend „next generation security".

W przypadku firewalli w urządzeniach nowej generacji filtrowanie w warstwie sieciowej zamieniono na filtrowanie na poziomie aplikacji. Oprócz tego nowe systemy przeprowadzają dogłębną kontrolę pakietów i inspekcję szyfrowanych sesji SSL, dając w miarę pełny wgląd w ruch sieciowy. Aby zwiększyć skuteczność detekcji zagrożeń, dostawcy w ostatnich

latach dodawali do swych rozwiązań kolejne funkcje, m.in. zaprzęgając do zadań analitycznych moc obliczeniową chmury. W przypadku ochrony przed włamaniami do sieci typu IPS (Intrusion Prevention System) „next generation security" wiąże się z uwzględnieniem kontekstu ciągłych zmian w sieci i dostosowywaniem się do nich. Z kolei nowe antywirusy muszą odpowiadać na zupełnie nowy sposób tworzenia złośliwego oprogramowania. Staje się ono coraz bardziej specjalizowane i polimorficzne, a więc niewykrywane przez rozwiązania bazujące wyłącznie na sygnaturach.

– *Ewolucja zagrożeń sprawiła, że aby zminimalizować ryzyko ataku, należy zbudować jak najbardziej kompletny ekosystem ochrony. Sam antywirus czy zwykły firewall już nie wystarczają. Muszą być wzmocnione przez dodatkowe, wyspecjalizowane rozwiązania do ochrony przed konkretnymi zagrożeniami* – twierdzi Mariusz Rzepka, dyrektor regionalny Fortinet na Polskę, Białoruś i Ukrainę.

W takim ekosystemie ochrony współczesnej sieci firmowej podstawą powinien być wydajny firewall nowej generacji albo – w przypadku mniejszych firm – rozwiązanie zintegrowane, czyli UTM (Unified Threat Management). Łączy on w sobie szereg funkcji: oprócz firewalla i antywirusa ma wbudowany system zapobiegający włamaniom IPS, mechanizm filtrowania stron WWW i wiele innych. Ze względu na swoją uniwersalność UTM-y są popularne wśród firm z sektora MSP. W większych sieciach ochrona przez firewall nowej generacji może być wzmocniona przez zastosowanie dedykowanych rozwiązań do zabezpieczania poczty elektronicznej, aplikacji webowych oraz do obrony przed specjalizowanymi atakami APT (użycie techniki sandboxingu) czy DDoS.

– *Ważne jest, aby rozwiązanie chroniące przed różnymi formami zagrożeń mogło być rozbudowywane o kolejne, bardziej zaawansowane elementy zabezpieczeń* – podkreśla Mariusz Kochański, dyrektor działu sieciowego w Veracompie.

> W dużych firmach rozwiązania UTM nie są wystarczająco skuteczne.

Treści pod kontrolą

Coraz większego znaczenia nabiera filtrowanie treści WWW w przedsiębiorstwach. Z jednej strony wymuszają to regulacje prawne, ponieważ pracodawca odpowiada za to, co jest pobierane z Internetu i przechowywane na służbowych komputerach (gdy pracownik pobrał treści niedozwolone, np. dziecięcą pornografię, to nie tylko on, ale i firma poniesie konsekwencje prawne).

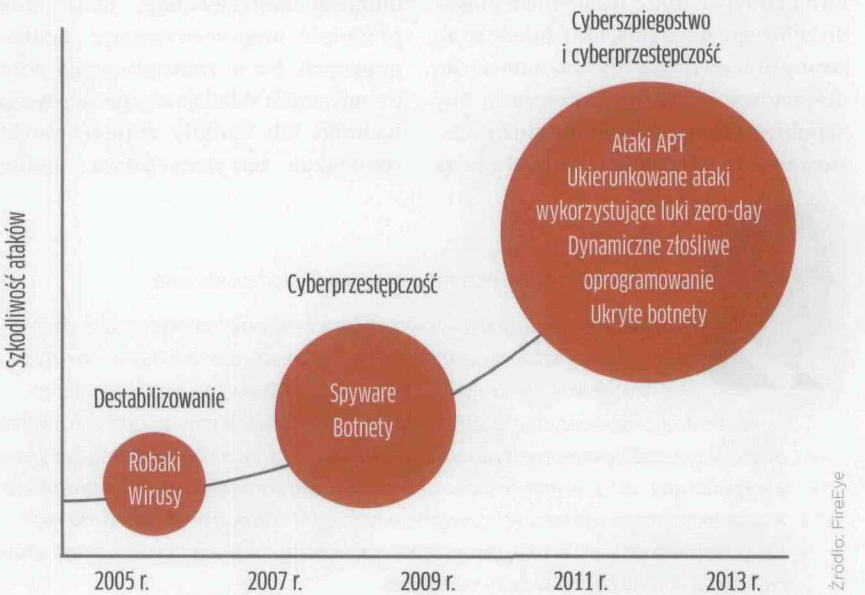
Z drugiej strony bardzo istotna jest kwestia produktywności pracowników. Przy czym zupełne zablokowanie dostępu do określonych stron przekłada się na niezadowolenie prrsolenu firmy. Znacznie lepszy efekt daje świadomość pracowników, że monitorowane są czas i miejsca, jakie odwiedzają w Internecie. Dzięki temu raczej nie będą spędzać większości swojego czasu w biurze np. na rozwijaniu najrozmaitszych aktywności na portalach społecznościowych.

– *Oprócz regulacji prawnych i kwestii produktywności pracowników trzeba wziąć pod uwagę przede wszystkim to, że Web jest najczęściej wykorzystywanym kanałem do rozsyłania złośliwego oprogramowania, wykorzystywanego następnie do ataków. Dlatego kontrola* →

Michał Kraut
konsultant rozwiązań systemów bezpieczeństwa, Cisco Systems

Firewall nowej generacji nie załatwia wszystkiego. Ważne jest też dołożenie specjalistycznych systemów ochrony stron web oraz poczty – te kanały komunikacji zdecydowanie dominują dziś w firmach. Dlatego przedsiębiorstwa powinny opierać swoje zabezpieczenia sieci na odpowiedniej kombinacji tych trzech elementów. Dodatkowo ważne jest posiadanie takich narzędzi, jak IPS czy sieciowy antywirus, które podejmują działanie, gdy atak już przełamie zabezpieczenia.

Ewolucja zagrożeń i ataków



Źródło: FireEye