



Ochrona treści

- niebezpieczeństwo czyha w sieci

Poniedziałkowy poranek, 9.00, typowy początek ciężkiego tygodnia pracy w biurze. Wśród niechcianych wiadomości znajdujesz reklamy oraz podejrzane e-maile przypominające korespondencję biznesową z załącznikami, która nakłania do odwiedzenia nieznanymi Ci stron. Jest też i poczta, która wykorzystując socjotechnikę, próbuje zwabić Cię na strony zawierające złośliwe obiekty. Konstruktorów takich wiadomości interesuje wyłącznie kradzież wrażliwych dla firmy danych. Ekspertki szacują, że obecnie ponad 10 000 stron dziennie jest infekowanych złośliwym kodem - dwukrotnie więcej niż na początku roku. Firmy dopiero teraz zdają sobie sprawę, jak istotna jest ochrona firmowej sieci przed groźną zawartością wnikałą poprzez pocztę elektroniczną oraz internet.

Jeśli wierzysz, że zabezpieczenie sieci jedynie przed wiadomościami spamowymi, wirusami oraz atakami phishingowymi stanowi wystarczającą ochronę, jesteś w błędzie. Produktom zabezpieczającym coraz trudniej jest rozpoznawać triki wykorzystywane przez atakujących sieci firmowe, w rezultacie trudniej im również zapobiegać samym atakom. Realnym zagrożeniem jest m.in. zawartość szyfrowanego ruchu SSL, serwisów XML oraz RSS, które nie dają się monitorować z wykorzystaniem konwencjonalnych rozwiązań bezpieczeństwa.

Ochrona treści jako element zintegrowanej strategii bezpieczeństwa oraz dostępności

Rośnie popyt na rozwiązania ochronne dedykowane dla konkretnych



sieci. Rośnie również liczba, rozmiar i złożoność samych sieci. W efekcie przemysł IT dostarcza na rynek różne komponenty ochronne dla poszczególnych obszarów wymagających zabezpieczenia – od rozwiązań zwalczających programy szpiegowskie, przez aplikacje antywirusowe, filtry anty-spamowe oraz IPS/IDS, aż po programowe i sprzętowe firewalles. W praktyce oznacza to, że firma pragnąca zapewnić sobie skuteczną ochronę musi korzystać z wielu rozwiązań różnych producentów. Pojawia się wtedy problem zintegrowania poszczególnych komponentów, które często okazują się wobec siebie niekompatybilne, przez co wyjątkowo trudno jest stworzyć jeden, homogeniczny

i skuteczny system bezpieczeństwa. Ideałem byłoby stworzenie systemu, który uniemożliwiałby wykorzystanie luk w systemie podczas ataków oraz dostarczałby pełnej informacji o sieci administratorowi odpowiadającemu za bezpieczeństwo. Jednak do ideału mogą zbliżać się jedynie zamożne firmy, które stać na ogromne wydatki zarówno na odpowiednio przeszkolony personel, jak i nowoczesną infrastrukturę.

Rozsądniejszym i znacznie wydajniejszym sposobem na zapewnienie sieci stosownej ochrony wydaje się implementacja zunifikowanej strategii bezpieczeństwa. Charles Kolodgy z International Data Corporation (IDC) jako pierwszy zdefiniował ten

Klaus Gheri, CTO oraz współzałożyciel firmy phion AG

Przed dołączeniem do zespołu phion AG pracował na Uniwersytecie w Innsbrucku jako profesor nadzwyczajny teorii fizyki. W phion odpowiada za zarządzanie produktem oraz rozwój firmy. Odegrał kluczową rolę podczas projektowania i rozwoju rozwiązania phion netfence, w szczególności systemu phion OS. Klaus Gheri posiada tytuł doktora fizyki Uniwersytetu w Auckland.

termin w 2004 r. Dzisiaj pojęcie to dotyczy w szczególności koncepcji Unified Threat Management (UTM). Wielu rynkowych graczy wykorzystuje jednak termin UTM nieprawidłowo, jako synonim urządzenia do zabezpieczania sieci typu „wszystko w jednym pudełku”. Takie pojmowanie UTM może być prawidłowe w małych firmach, w których wiele komponentów bezpieczeństwa IT udaje się łączyć w jednym urządzeniu. Umożliwia to racjonalizację kosztów oraz zmniejszenie stopnia skomplikowania infrastruktury. Tym samym wydatki pozostają na niezmiennym,

akceptowalnym poziomie, a popyt na zintegrowaną strategię zostaje zrealizowany. Jednak w większych przedsiębiorstwach nie można stawić znaku równości pomiędzy UTM a zabezpieczeniem określanym jako „wszystko w jednym pudełku”. Firmy posiadające rozbudowane sieci, z wieloma lokalizacjami oraz komponentami bezpieczeństwa, wykorzystują koncepcję UTM do stworzenia i wdrożenia zintegrowanej strategii ochrony z centralnym zarządzaniem dla całej infrastruktury IT w firmie. Najważniejszymi elementami rozwiązania UTM są:

- scentralizowane zarządzanie i uniwersalna interoperacyjność;
- równowaga pomiędzy bezpieczeństwem a potrzebami;
- optymalny zwrot z inwestycji (ROI).

W pełni zintegrowana komunikacja - bezpieczeństwo, dostępność oraz inteligentne zarządzanie

Firma phion AG, jeden z czołowych w Europie dostawców rozwiązań do ochrony komunikacji i zasobów sieci firmowych, realizuje najważniejsze potrzeby z dziedziny bezpieczeństwa, dostępności oraz inteligentnego zarządzania poprzez rodzinę produktów netfence. Bazując na koncepcji UTM, phion dostarcza rozwiązania ochrony treści, które gwarantują centralną administrację oraz poprawną współpracę poszczególnych komponentów sieci od samego początku. Rozwiązania firmy phion to:

- firewall;
- potężna platforma ochrony treści połączona z najnowszą generacją skanera antywirusowego;
- kompleksowa ochrona poczty elektronicznej.

Zagrożenia z sieci są coraz bardziej zjadłe, w rezultacie rośnie znacznie ochrona treści. Z drugiej jednak strony, ochrona treści nadal jest tylko jednym z komponentów całej strategii bezpieczeństwa firmy, której sukces zależy od efektywnej współpracy pomiędzy wszystkimi jej elementami. Dzięki integracji rozwiązań phion z pokaźną grupą produktów z kategorii bezpieczeństwa oraz infrastruktury sieci możliwa jest współpraca ze wszystkimi komponentami sieci firmowej.

*Autor: Dr Klaus Gheri, CTO
w firmie phion AG*

Konferencja PHION 2008 w Warszawie pod patronatem CIO

Już 11 września w warszawskim hotelu Marriott odbędzie się konferencja PHION 2008, poświęcona systemowi zarządzania bezpieczeństwem komunikacji poprzez sieci VPN - phion netfence. Spotkają się na niej administratorzy IT największych firm. To największa od dwóch lat konferencja austriackiej firmy phion w Polsce. „CIO Magazyn Dyrektorów IT” został patronem medialnym wydarzenia. Firma phion jest znana w Europie ze stworzenia unikalnego systemu zarządzania bezpieczeństwem komunikacji pracującego dla dużych wieloodziałowych koncernów i instytucji europejskich, takich jak produkujący samoloty Airbus koncern EADS, grupa przemysłu naftowego OMV czy też STRABAG - czołowa grupa branży budowlanej w Europie. Konferencja PHION 2008 organizowana 11 września br. w warszawskim hotelu Marriott będzie poświęcona nowościom w systemie ochrony komunikacji i zasobów sieciowych phion netfence. Udział w konferencji jest bezpłatny. Szczegółowy harmonogram oraz formularz zgłoszeniowy można znaleźć na stronie internetowej dystrybutora: <http://www.dagma.com.pl>.