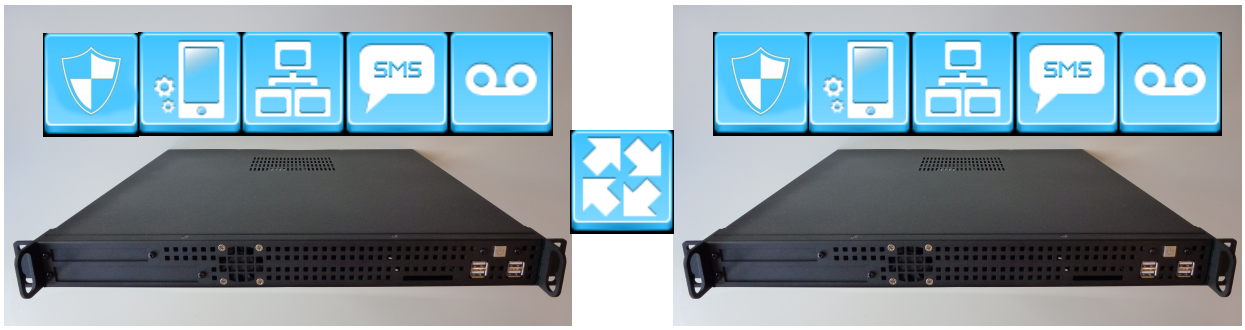
NEWSLETTER Lipiec 2017

W dobie realnych zagrożeń atakami cybernetycznymi na infrastrukturę teleinformatyczną administratorzy (użytkownicy) oraz producenci systemów telekomunikacyjnych zastanawiają się jak skutecznie chronić swoje urządzenia.
Niektórzy nawet z nostalgią spoglądają w przeszłość do klasycznych central telefonicznych z polem komutacyjnym lub być może dalej do central elektromechanicznych gdzie atak cybernetyczny w obecnej postaci byłby niemożliwy.
Oczywistym jest, że nie ma powrotu do starych rozwiązań w szczególności że nie sprostają one wymogom współczesnej zunifikowanej komunikacji.

Co za tym robić, jak się bronić?

Podstawą jest świadomość zagrożeń, właściwe praktyki oraz zapewnienie maksymalnego bezpieczeństwa wynikającego z dostępnej wiedzy oraz technologii.

Ochrona danych wrażliwych, stosowanie trudnych haseł, stosowanie nietypowych portów dla podstawowych protokołów sieciowych (http, ftp, ssh itp.) , szyfrowanie lub sesje vpn, stosowanie firewall lub specjalistycznych Session Border Controllers, aktualizacja oprogramowania, a w przypadku udanego ataku zapewnienie aby infrastruktura telekomunikacyjna (krytyczna) mogła działać, przywracając jej stan sprzed ataku.

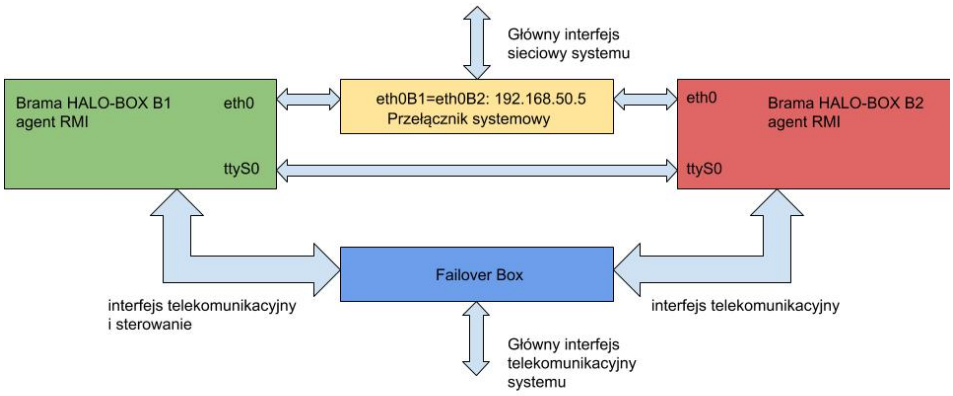


HALO-SKY.NET wpisując się w obecne trendy przygotował rozwiązanie zwiększające bezpieczeństwo cybernetyczne oferowanych bram halo-box.

Halo-Box Guard to system redundanty bram Halo-Box, w którym zastosowano tryb chroniony.
Polega on na tym że rezerwowa brama jest całkowicie odizolowana od zagrożonej atakiem infrastruktury teleinformatycznej tzn. nie posiada bezpośredniego podłączenia IP.
Uniemożliwia to infekcję złośliwym oprogramowaniem lub nieautoryzowaną zmianę konfiguracji bramy rezerwowej w przypadku udanego ataku.

Rezerwowa brama halo-box nadzoruje pracę bramy głównej poprzez zaimplementowany w bramach interfejs szeregowy, przez który dedykowanym protokołem komunikują się agenci RMI.
Nowe oprogramowanie agentów RMI zostało wyposażone w dodatkowy tryb pracy chronionej, w którym nadzorowana jest aktywność administratora.
Próba wyłączenia procesów komunikacyjnych, aktywowanie zmienionej konfiguracji, czynności wymagające uprawnień roota na bramie głównej powodują wygenerowanie alarmu.
Alarm ten przekazywany jest do administratora systemu niezależnym kanałem komunikacyjnym.
Wówczas administrator może przełączyć system przywracając jego funkcjonalność po wykonaniu czynności sprawdzających.

Istnieje również tryb autonomiczny w którym brama rezerwowa przełącza się automatycznie.



Aby zapewnić szczególną ochronę brama rezerwowa może przełączyć jedynie interfejsy telekomunikacyjne (E1) udostępniając zasoby w ramach np. sieci rezerwowej.

Halo-Box Guard można implementować na wszystkich zainstalowanych systemach Halo-Box
W przypadku systemów redundantnych wystarczy jedynie zmienić sposób połączenia i zainstalować nowe oprogramowanie agenta RMI.
W przypadku bram pojedynczych należy rozbudować do systemu redundantnego.
Halo-Box Guard jest również dostępny domyślnie na wszystkich nowych systemach Halo-Box.

Oferujemy również przetestowane markowe Session Border Controllers.

Szczegółowych informacji na temat przedstawionego rozwiązania udziela:

Adam Kabot
email: adam.kabot@halo-sky.net
tel. +48 884769520, kom. +48 697988391

Arkadiusz Waleczek

arkadiusz.waleczek@halo-sky.net
tel. +48 884769520 , kom. +48 794168214
www.halo-sky.net