Japońska Twierdza z Hitachi Vantara

Przedstawiona na „Grafice” Japońska Twierdza jest niedoścignionym wzorcem obronności przed zagrożeniami z zewnątrz. W dzisiejszych czasach mamy znacznie więcej problemów przed którymi należy sie chronić. Zararówno przed zewnętrznymi jak i wewnętrznymi. Są nimi pożary, trzęsienia ziemi, powodzie, tajfuny, a ostatnio niedaleko naszych granic mawet ataki rakietowe. Najczęstszymi atakami są jednak nadal ataki prowadzone przez cyberprzestępców, znane pod nazwą „ransomware”. Maja one na celu włamanie sie do centrum informatycznego i przejecie kontroli nad systemem oraz rozpoczęcie procesu szantarzu finansowego.

Obroną na ataki tego typu ze względu na ich specyfike – mogą byc tylko procesy reaktywne – odpowiadające na skutki tych ataków w taki sposób, by zasięg i ich nastepstwa były jak najmniejsze i wyeliminowane z systemów jak najszybciej.

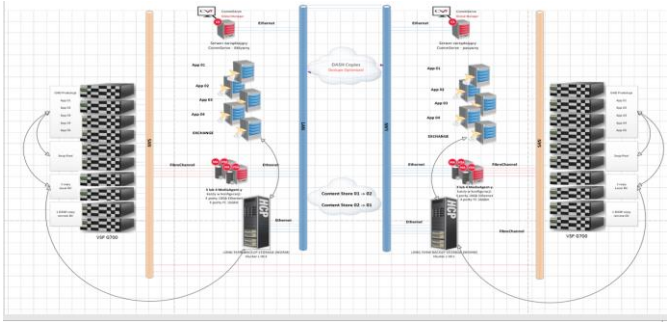
I tu nalezy odnieśc się do podstawy budowania bezpieczeństwa systemów Informatycznych. Każde Przedsiebiorstwo posiada Księgę Zarządzania, a w niej jeden Dział dotyczy Bezpieczeństwa Ogólnie Pojętego, w którym zawiera się bezpieczeństwo systemów IS/IT. Wytycznymi Bezpieczeństwa są parametry RTO i RPO. Wskaźnik RPO (Recovery Point Objective) określa dopuszczalną ilość utraconych danych i maksymalny akceptowalny czas pomiędzy wystąpieniem awarii, a backupem danych. Wskaźnik RTO (Recovery Time Objective) określa jak szybko infrastruktura IT jest przywrócona do pracy po wystąpieniu awarii lub innego incydentu. To własnie RPO i RTO mają bezpośredni wpływ polityke BCM (Business Continuity Management), dzięki której posiadamy procedury utrzymania produkcji/zarobków w ciągłym ruchu.

Poza procesami biznesowymi należy się zastanowić również nad architekturą całego IS/IT, i tu nalezy przede wszystkim wyeliminować Pojedyńcze Punkty Awarii (SPOF – Single Point of Failure), które przy minimalnym niedopatrzeniu mogą byc początkiem wielkiej awarii.

Hitachi Vantara od kilkudziesięciu lat dostarcza do klientów rozwiazania które dają 100% gwarancje dostepu do danych, a dodatkowo wspomaga swoich klientów w planowaniu, wdrażaniu, utrzymywaniu i

rozwoju systemów krytycznych dla wielu przedsiębiorstw. Zrównowazone inwestycje, przy efektywnym nakładzie finansowym w technologie daje bardzo pozytywne odczucia każdemu, kto korzysta z takich systemów. Japońska technologia jest znana z tego, że dobrze wdrożona i utrzymywana, działa bezprzerwowo dłużej niż zakłada na to gwarancja producenta.

Proponuję by architektura Japońskiej Twierdzy zawierała przynajmniej dwie Serwerownie.



Kazda z nich powinna zawierać:

1. Klaster Blokowy

Global Active Device-Streach Cluster : bardzo wydajny system zapisu zmian w obu lokalizacjach, z wbudowanymi funkcjonalnościami bezpiecznych i niezmiennych Snaphotów (Shadow Copy, Thin Image) a na nim Hypervisor wirtualizujący systemy operacyjne.

2. Klaster Objektowy

A na nim kontent obiektów/plików niestrukturalnych z mozliwością Kwalifikacji i Klasyfikacji treści, z wbudowanymi politykami podnoszącymi bezpieczeństwo i niezmiennność danych zimnych(archiwalnych) WORM (Write Once Read Many). Tu dodatkowo umieszczamy Złotą Kopie Selektywną Pełną (z dostępem typu AirGAP) całego systemu IS/IT by miec pewność powrotu po Awarii, nawet takiej gdzie będziemy gasić pożar po ataku Ransomware.

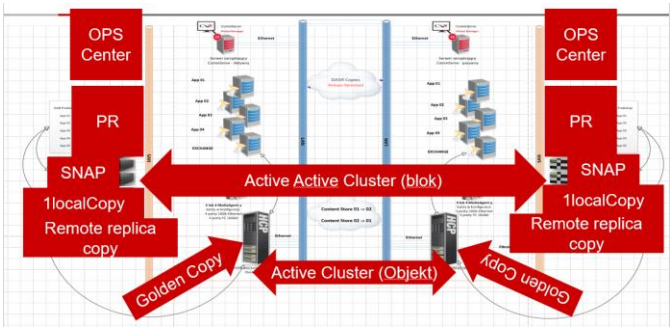
3. System Backupowy HDPS

(HDPS) Hitachi Data Protection Suite – pozwalający na utworzenie systemu do zabezpieczeń, który nie posiada pojedynczego punktu awarii, który pozwala na zdefiniowanie wyizolowanej sieci backupowej, oraz zdefiniowanie polityk RPO i RTO dla dowolnych zasobów zgodnie z Polityką Bezpieczeństwa w Waszym Przedsiębiorstwie.

4. System Zarzadzania, Monitorowania, Automatyzacji i Bezpieczeństwa

OPS Center: to rozwiązanie wspomagajace w codziennych zadaniach administratorów IS/IT, jednocześnie pozwalający na tworzenie raportów SLA dla poszczególnych usług minitorowanych w tym systemie.

Poziom zabezpieczenia w wyżej wymienionej architekturze przedstawia sie następująco:



Dodatkowym atutem Japońskiej Twierdzy jest łatwa skalowalność (dodawanie pojemności lub wydajności do poszczególnych elementów architektury) bez utraty dostępu do danych. Oraz łatwość odpowiedzi na pytania Audytorów którzy co roku maja obowiązek sprawdzania poziomu zabezpieczeń w firmie nie tylko systemów IS/IT.

Każdemu z was życzę bezprzerwowego działania systemów IS/IT, w którym jest czas na planowanie, elastyczny rozwój, oraz bezproblemowe utrzymywanie.

Mniej gaszenia pożarów (reaktywność) ma bezpośreni wpływ na profilaktykę (proaktywność) i dzieki takiemu podejściu, mamy czas na ważne rzeczy.

Pozdrawiam

Autor Piotr