

DLACZEGO SAMORZĄDY POWINNY TROSZCZYĆ SIĘ O BEZPIECZEŃSTWO?

Brak odpowiedniego poziomu bezpieczeństwa utrudnia realizację nadrzędnych celów samorządów: zwiększania efektywności usług, poprawy bezpieczeństwa publicznego i rozwoju gospodarczego.

- Szybko rozprzestrzeniające się wirusy i robaki, włamania oraz ataki hackerów blokujące dostęp do usług, (ang. Distributed Denial of Service — DDoS) mogą unieruchomić sieci, uniemożliwiając ich użycie w celach związanych z bezpieczeństwem publicznym i usługami dla mieszkańców; dodatkowo rosną koszty, co jest związane z przywracaniem funkcjonowania w zainfekowanych sieciach i komputerach.
- Poufne dane obywateli i organów samorządowych mogą zostać ujawnione w trakcie ich przesyłania przez Internet za pomocą połączenia przewodowego lub bezprzewodowego, co narusza bezpieczeństwo i poufność usług.
- Mieszkańcy obawiają się zawierania oficjalnych lub prawnie wiążących transakcji za pomocą skradzionej tożsamości lub bez wymaganego upoważnienia.

Są to wyraźnie widoczne i politycznie niebezpieczne sytuacje, które mogą nadszarpanąć zaufanie publiczne do władz samorządowych. Jak stwierdzono w raporcie RAND Europe, pt. *Benchmarking Security and Trust in Europe and the US*: „...powszechnie uznaje się, że brak zaufania do usług świadczonych drogą elektroniczną jest istotną barierą na drodze do rozwoju modelu e-administracji”.

JAKIM WYZWANIOM NALEŻY SPROSTAĆ?

- Unikanie sytuacji w których dochodzi do „utraty zaufania”.
- Zwiększenie efektywności usług dzięki inteligentnym telecentrom, rozwiązaniom wspomagającym pracę zespołową oraz rozwiązaniom dla pracowników mobilnych.
- Poprawa bezpieczeństwa publicznego dzięki kamerom bezprzewodowym, nadawaniu ostrzeżeń i zdalnemu dostępowi do aplikacji policyjnych.
- Przyciąganie inwestycji dzięki bezpiecznym serwisom samoobsługowym, które świadczą usługi dla mieszkańców i udostępniają w bezpieczny sposób, drogą elektroniczną, procedury administracyjne.

ZINTEGROWANE ROZWIĄZANIA ZABEZPIEZAJĄCE dla JST, FIRMY CISCO SYSTEMS

Rozwiązania Cisco Integrated Security dla administracji publicznej stanowią podstawę strategii Cisco samodzielnie broniącej się sieci (ang. Cisco Self-Defending Network), która łączy w sobie takie funkcje jak:

- *Obrona przed zagrożeniami* — ochrona sieci przed zagrożeniami, włamaniami i blokadą w świadczeniu usług, poprzez powstrzymywanie infekcji oraz izolowanie urządzeń, które zachowują się w sposób nietypowy (wykorzystanie zjawiska analizy anomalii ruchu danych).
- *Bezpieczna łączność* — ochrona poufnych danych i plików przed nieautoryzowanym dostępem. Zapewnienie samorządom zgodności z przepisami dotyczącymi poufności danych, sformułowanymi przez polskie ustawodawstwo.
- *System zarządzania zaufaniem i tożsamością* — umożliwienie bezpiecznego dostępu do sieci e-urzędu dla mieszkańców, kontrahentów, pracowników mobilnych i osób niepełnosprawnych, pracujących z domu.



Strategia Self-Defending Network jest oparta na trzech zasadach:

- *Zasada integracji* — każdy element sieci pełni funkcje obronne.
- *Zasada współpracy* — różne komponenty sieci współpracują ze sobą, tworząc spójny - kompleksowy model ochrony.
- *Zasada adaptacji* — sieć automatycznie powstrzymuje nowe rodzaje zagrożeń, gdy tylko się pojawiają, poprzez wykrywanie nietypowego zachowania sieci lub aplikacji i stosowanie mechanizmów sterowania siecią.

Dzięki połączeniu tych trzech zasad, sieci samorządowe zyskują właściwości niezbędne do skutecznego świadczenia usług i zapewnienia bezpieczeństwa publicznego, tj.: ciągła praca, powszechny dostęp do usług, kontrola dostępu, inteligentna analiza aplikacji, ochrona przed atakami typu „day zero” i powstrzymywanie infekcji.

ZALETY ZINTEGROWANYCH ZABEZPIECZEŃ

Zwiększona efektywność usług

Dzięki bezpiecznej, zawsze dostępnej sieci samorządy ułatwiają współpracę między różnymi organizacjami. Dochodzi do rozszerzenia zasięgu usług na mieszkańców w odległych obszarach i pracowników zdalnych. Dla transakcji realizowanych drogą elektroniczną jest zapewniony taki sam poziom zaufania, bezpieczeństwa oraz waga prawna, jak w przypadku transakcji „papierowych”.

Poprawa bezpieczeństwa mieszkańców

Samorządy mogą poprawić bezpieczeństwo mieszkańców, zapewniając ciągłość świadczenia usług, umożliwiając osobom, które jako pierwsze reagują na dane zdarzenie, lepsze rozeznanie w sytuacji dzięki transmisji obrazu w czasie rzeczywistym, a także chroniąc poufność danych osobowych obywateli i informacji samorządu.

Rozwój gospodarczy

Rozwiązania Cisco Integrated Security pobudzają dynamiczny rozwój gospodarki społeczności, gdyż pozwalają samorządom zapewnić całodobowy dostęp do informacji administracyjnych, zaoferować bezpieczne usługi elektroniczne, a także zwiększyć dostępność wykwalifikowanej kadry dzięki obsłudze elastycznych stanowisk pracy i telepracowników.

DLACZEGO CISCO?

- Współpraca z innymi firmami z branży w celu zbudowania prewencyjnej, samodzielnie broniącej się sieci — Self-Defending Network.
- Elastyczne, ekonomiczne wdrażanie usług bezpieczeństwa oraz zarządzanie tymi usługami.
- Bezproblemowa integracja sieci IP z usługami zabezpieczeń i dotychczasową infrastrukturą.
- Konwergentne, zintegrowane rozwiązanie pochodzące od jednego dostawcy.
- Skalowalna, globalnie rozproszona struktura, która może dostosowywać się do przyszłych potrzeb.
- Najniższy całkowity koszt posiadania (TCO) i najwyższy zwrot z inwestycji (ROI).

Zintegrowane zabezpieczenia dla Jednostek Samorządu Terytorialnego — przegląd

KOMPONENTY SIECI SELF-DEFENDING NETWORK

Ochrona i kontrola punktów końcowych sieci

- Cisco Security Agent
- Network Admission Control (NAC)
- Identity-based networking (IBNS)
- Funkcja „Are You There?” (AYT) sieci VPN
- Rozszerzenia bezprzewodowe zgodne z urządzeniami Cisco

Ochrona infrastruktury sieciowej

- Progi wykorzystania procesora/pamięci
- Funkcja Control Plane Policing
- Mechanizm Cisco AutoSecure
- Zabezpieczenia portów, podglądanie protokołu DHCP, dynamiczna inspekcja protokołu ARP (Address Resolution Protocol), IP Source Guard
- Cisco Structured Wireless-Aware Network (SWAN)

Bezpieczna, elastyczna łączność

- Sieci VLAN
- Dynamiczna, wielopunktowa sieć VPN
- Easy VPN
- Sieć VPN oparta na protokole SSL
- Obsługa protokołów GRE (Generic Routing Encapsulation) / IPSec (IP Security)
- Pakiet zabezpieczeń Cisco dla komunikacji bezprzewodowej

Inspekcja i kontrola ruchu

- Inspekcja i egzekwowanie reguł w zależności od aplikacji
- Weryfikacja protokołu
- Elastyczne wdrażanie zapory i systemu zapobiegania włamaniom (Intrusion Prevention System — IPS)
- Ochrona przed atakami typu DDoS.

Dynamiczna ochrona oparta na współpracy

- Wykrywanie anomalii w sieci
- Cisco NetFlow i Cisco Network-Based Application Recognition (NBAR).
- Aktywne zapobieganie włamaniom
- Analiza zagrożeń i reagowanie na nie
- Ochrona przed atakami typu DDoS

SŁOWNIK ROZWIĄZAŃ ZABEZPIELAJĄCYCH FIRMY CISCO

Cisco Access Control Server — produkt zwiększający bezpieczeństwo dostępu dzięki umożliwieniu uwierzytelniania, przyznawania dostępu użytkownikom i administratorom oraz kontroli reguł za pomocą scentralizowanej infrastruktury do obsługi tożsamości. <http://www.cisco.com/go/acs>

Cisco Security Agent — komercyjny pakiet oprogramowania do zarządzanej ochrony punktów końcowych, takich jak komputery osobiste i serwery. Wykorzystuje wielowarstwową, kontekstową analizę zachowań do identyfikowania i powstrzymywania niewłaściwej aktywności systemów. Aktualizacje sygnatur nie są wymagane. <http://www.cisco.com/go/csa>

Cisco Trust Agent — klient do systemu NAC, przekazujący właściwości urządzeń do ruterów obsługujących NAC (patrz „Network Admission Control”). <http://www.cisco.com/go/cta>

Identity Based Networking Services (IBNS) — infrastruktura uwierzytelniania, autoryzacji i rozliczania użytkowników (Authentication, Authorisation and Accounting — AAA), zarządzająca dostępem użytkowników i administratorów do sieci. Wykorzystuje standard 802.1x oraz kompleksową strukturę rozwiązania. <http://www.cisco.com/go/ibns>

Intrusion Detection System (IDS) — system zapewniający wykrywanie znanych zagrożeń w samej sieci. <http://www.cisco.com/go/ids>

Intelligent Information Network (IIN) — koncepcja firmy Cisco przewidująca integrację technologii, aplikacji biznesowych oraz nowych architektur. <http://www.cisco.com/go/intelligentnetworking>

Intrusion Prevention System (IPS) — system zapewniający inteligentne wykrywanie znanych i nieznanych zagrożeń w sieci oraz zapobieganie im. <http://www.cisco.com/go/ips>

Network Admission Control (NAC) — systemowe rozwiązanie zapewniające egzekwowanie zasad bezpieczeństwa, ochronę oraz kontrolę przestrzegania reguł w punktach końcowych. Egzekwuje przestrzeganie reguł dostępu w punktach końcowych (zezwoleń, odrzucenie, kwarantanna) na podstawie profili znajdujących się na serwerze Cisco ACS oraz na serwerach dostarczonych przez partnerów uczestniczących w programie NAC. <http://www.cisco.com/go/nac>

Network Infection Containment (NIC) — produkt ograniczający skutki infekcji dzięki skróceniu czasu potrzebnego na identyfikację i odizolowanie zainfekowanych systemów oraz oczyszczenie ruchu sieciowego. <http://www.cisco.com/go/ti>

Self-Defending Network (SDN) — opracowana przez firmę Cisco koncepcja ochrony sieci i połączonych zasobów. Jest oparta na trzech zasadach: integracji, współpracy i adaptacji. <http://www.cisco.com/go/selfdefend>

Trust and Identity Solutions (T&I) — zestaw rozwiązań umożliwiających przekazywanie praw dostępu do sieci na podstawie reguł, stanu bezpieczeństwa oraz profilu użytkownika lub urządzenia. <http://www.cisco.com/go/ti>

Threat Defence System (TDS) — zestaw rozwiązań zapewniający prewencyjną ochronę przed znanymi i nieznanymi atakami w sieci oraz w jej punktach końcowych. <http://www.cisco.com/go/tds>

MATERIAŁY

Samorządy

<http://www.cisco.pl/jst>

<http://www.cisco.com/govnow>

<http://www.cisco.com/go/localgov>

Cisco Security

<http://www.cisco.com/go/security>

<http://www.cisco.com/go/selfdefend>

<http://www.cisco.com/securitynow>

Słownik terminów branżowych związanych z bezpieczeństwem

<http://www.nxtbook.net/live/cisco/securityglossary/index.html>