Elementy infrastruktury i cyberbezpieczeństwa

Marcin Piekarek
Dyrektor
Centrum Informatyki Statystycznej

Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Ochrona brzegowa

Już przy pierwszym podłączeniu GUS do Internetu (w 1997 roku) uwzględnione zostały aspekty bezpieczeństwa.

- **2000** - Zapora brzegowa – pierwsza zapora sieciowa Raptor w GUS
- **2004** - Zapora brzegowa Checkpoint z dodatkowymi modułami IDS *(ang. Intrusion Detection System) – RealSecure SiteProtector Proventia*
- **2010** - Cisco ASA – zapora brzegowa wykorzystywana do zabezpieczenia połączeń VPN
- **2011** - IPS *(ang. Intrusion Prevention System) – HP TippingPoint*
- **2013** - Checkpoint DDoS Protector – system zabezpieczeń przed atakami DDoS
- **2018** - Ochrona DDoS przeniesiona została jako usługa na dostawców Internetu

Ochrona poczty elektronicznej

Pierwszy system pocztowy zbudowany był na Linuxie w roku 1995. Obsługiwał pocztę wewnętrzną i zewnętrzną dla części pracowników.

- **2000** - Implementacja właściwego systemu pocztowego, który obejmował 51 serwerów, 49 w WUS i dwa centralne, komunikacyjne w GUS. Antywirus Sophos
- **2001** - Centralizacja usług pocztowych - Pierwsze zabezpieczenie w 2001, antywirus z możliwością filtrowania IP (McAfee - WebShield) – rozwiązanie wzmocniło serwer Exchange
- **2005** - Pierwsze urządzenie typu Mail Gateway – ASSP (*ang. Anti-Spam SMTP Proxy*)
- **2007 - 2015** - ORF Fusion – System ochrony serwerów Microsoft Exchange
- **2015** - McAfee e-mail security + oprogramowanie ESET e-mail security z ochroną antyspamową i antywirusową
- **2018** - Trend Micro IMSVA + oprogramowanie ESET e-mail security z ochroną antyspamową i antywirusową
- **2021** - Wdrożenie nowego systemu ochrony poczty

Kontrola dostępu do Internetu

- **2000** - Zapora brzegowa Raptor umożliwiała udostępnienie połączenia do Internetu na podstawie adresów IP użytkowników
- **2004** - Oprogramowanie Surf Control Web Filter (od 2007 roku Websense). Umożliwiło filtrowanie adresów URL w treści stron
- **2007** - CheckPoint – Dostęp do Internetu z aktywnym modułem URL Filtering. Rozwiązanie uzupełniło istniejący MS ISA Server
- **2011** - Microsoft Forefront Threat Management Gateway zastąpił MS ISA Server
- **2018** - Citrix Proxy SVG
- **2021 –** Nowy system dostępu do Internetu z funkcjonalnością proxy

Ochrona stacji roboczych

Oprogramowanie antywirusowe

- **1998** - Centralnie zarządzany system antywirusowy Sophos
- **2001** - McAfee Virus Scan
- **2017** - Symantec Endpoint Protection

Advanced Threat Protection – Wdrożenie w ramach KSZBI

2022 – System klasy Endpoint Detection and Response – umożliwia zaawansowane wykrywanie i blokowanie szkodliwego oprogramowania na podstawie zarejestrowanych działań w systemie operacyjnym np. modyfikacja rejestru czy plików systemowych

Ochrona aplikacji webowych

- **2006** - Publikacja Form (później Portal Sprawozdawczy) i Portal Informacyjny przez Cisco Content Services Switch
- **2007 - 2008** – Publikacja (najpierw PKD2007, potem również inne aplikacje) przez ISA
- **2011** - Publikacja przez MS TMG (Microsoft Forefront Threat Management Gateway)
- **2015** - Publikacja Portalu Sprawozdawczego i Portalu Informacyjnego przez F5 Big-IP
- **2018** - Publikacja przez WAF Citrix ADC
- **2021** - Publikacja przez WAF (KSZBI)

Ochrona ruchu sieciowego w sieci wewnętrznej

- **2011** - IPS (*ang. intrusion prevention system*) – HP TippingPoint
- **2019** – Wdrożenie na potrzeby PSR2020 i NSP2021 New Generation Firewall. Segmentacja sieci i włączenie *deep inspection* z prewencją zagrożeń
- **2020** – Uruchomienie infrastruktury wirtualizacyjnej Vmware z funkcją mikrosegmentacji sieci z kontrolą dostępu na poziomie adresu i usługi

Kontrola dostępu do sieci

- **2015** - Direct Access – bezpośrednie połączenie VPN do infrastruktury
- **2015** - Kontrola dostępu 802.1X dla sieci bezprzewodowej
- **2018** - Port security – Zdecentralizowana kontrola dostępu do LAN
- **2019** - Rozbudowa kontroli dostępu 802.1X dla sieci przewodowej w budynku GUS
- **2018** - Portal Workspace – Zdalny dostęp do stacji roboczych i niektórych aplikacji Web
- **2020** - Always-On IPSec-VPN - Uruchomienie na bardzo dużą skalę pracy zdalnej w związku z pandemią COVID-19

Rozbudowa systemu kopii zapasowych w CPD

- Macierz dyskowa DELL Unity XT-680

  381 dysków twardych o łącznej
  przestrzeni użytkowej 516.9 TB (RAID 6)

Macierz jest komponentem systemu backupowego Veeam oferując przestrzeń roboczą wykorzystywaną podczas:

- tworzenia kopii zapasowych,
- tworzenia kopii migawkowych systemy wirtualizacyjnego Vmware.

Rozbudowa systemu kopii zapasowych w CPD

- Dwie biblioteki taśmowe Q-80 oraz 320 kaset taśmowych LTO-8 (po 12 TB każda)

Zakupione urządzenia uzupełniły infrastrukturę wirtualizacyjną zakupioną na potrzeby PSR2020 i NSP2021.

✓ Zwiększony poziom bezpieczeństwa danych i dostępności systemów.

Rozbudowa sieci bezprzewodowej

- Rozbudowa sieci bezprzewodowej – wdrożenie zakończone w styczniu 2022 r.

W ramach umowy wdrożono 60 punktów dostępowych, rozbudowując infrastrukturę sieci bezprzewodowej do 180 access pointów.

✓ Zwiększenie dostępności do sieci bezprzewodowej w GUS i Urzędach Statystycznych.

Rozbudowa sieci bezprzewodowej

Z uwagi na publiczny dostęp do medium transmisyjnego konieczne było zapewnienie właściwej kontroli dostępu do sieci zgodnej ze standardem 802.1X.

System kontroli dostępu do sieci bezprzewodowej uzupełnił istniejącą infrastrukturę teleinformatyczną zapewniając dla niej:

- Kontrolę dostępu do sieci przewodowej zgodną ze standardem 802.1X
- Wielopoziomową kontrolę dostępu do urządzeń sieciowy dla operatorów i administratorów

✓ Zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej.

Modernizacja systemu akceleracji

- Modernizacja systemu akceleracji

11 lutego 2022 uruchomiony został nowy system akceleracji ruchu w sieci WAN statystyki publicznej łączącej siedzibę GUS z Urzędami Statystycznymi oraz Zakładem CIS w Radomiu.

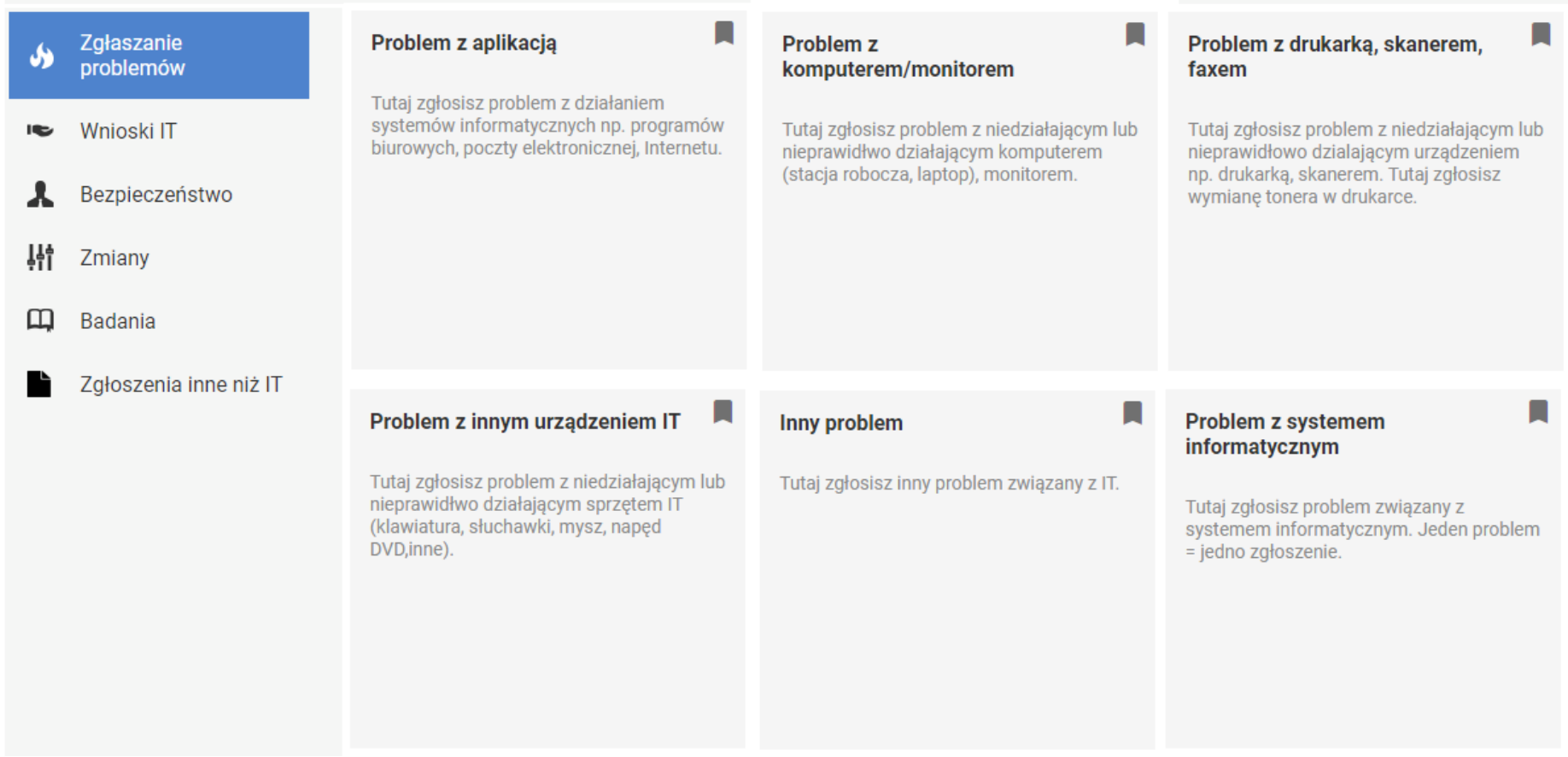
Zapewnienie akceleracji ruchu i ograniczenie jego nadmiarowości już u źródła pozwoliło na utrzymanie dotychczasowych przepustowości łącz telekomunikacyjnych pomimo wzrostu zapotrzebowania na pasmo.

✓ Bardziej efektywne administrowanie urządzeniami, zoptymalizowanie ruchu w sieci WAN.

System Serwis Desk

W ramach wdrożenia zaimplementowano procesy:

- Zgłoszenia awarii
- Zgłoszenia wniosków



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
GUS
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

System Serwis Desk

System rozbudowano o obsługę procesów przygotowanych w projekcie KSZBI.

- Wprowadzono obsługę incydentów bezpieczeństwa zgodnie z *Zasadami zarządzania incydentami bezpieczeństwa*
- Stworzono osobne procesy do obsługi incydentów teleinformatycznych, bezpieczeństwa środowiskowego i fizycznego
- Wprowadzono obsługę zgłoszeń dotyczących uprawnień do systemów zgodnie z *Zasadami Zarządzania Uprawnieniami*, dzięki czemu powstała ewidencja uprawnień dostępu do systemów
- Wprowadzono obsługę wniosków o zmianę zgodnie z *Zasadami zarządzania zmianą*

System Serwis Desk

Wcześniej w jssp ewidencja była prowadzona w sposób nieuporządkowany, w różnych narzędziach, a posiadane informacje o sprzęcie i oprogramowaniu miały różny zakres.

W ramach projektu przygotowano formularze opisu elementów konfiguracji zgodnie z opracowanymi w ramach projektu KSZBI.

Obecnie wszystkie elementy znajdują się w bazie CMDB (centralna baza konfiguracji).

Testy bezpieczeństwa

Testy penetracyjne

- Prowadzone od 2011 roku
- Black box testing – brak informacji o konfiguracji aplikacji i kodzie źródłowym.
- Testy manualne i zautomatyzowane
- Raport końcowy opisujący znalezione podatności, dowody istnienia luk, scenariusze ataku oraz zalecenia dotyczące poprawy systemu

W ramach prac projektowych

- Wymagania i rekomendacje dotyczące bezpieczeństwa informacji i ochrony danych osobowych w budowanych i modyfikowanych systemach i aplikacjach
- Rekomendacje dotyczące przeprowadzania testów bezpieczeństwa

Testy bezpieczeństwa cd.

Zadania zespołu testującego

Do zadań zespołu Centrum Informatyki Statystycznej przeprowadzającego testy należy:

- określenie zakresu realizowanych testów,
- zapoznanie się z funkcjonalnością aplikacji,
- przeprowadzenie testów penetracyjnych,
- opcjonalnie: analiza kodów źródłowych aplikacji oraz zawartości bazy danych wykorzystywanej przez aplikację,
- wykonanie raportu z przeprowadzonych testów bezpieczeństwa.

Wymagane jest, by przed produkcyjnym uruchomieniem, system został poddany testom bezpieczeństwa oraz posiadał dokumentację – raport po przeprowadzonych testach bezpieczeństwa.

Testy bezpieczeństwa cd.

Narzędzia

- OWASP ZAP – aplikacja open source do automatyzacji testów bezpieczeństwa rozwijana w ramach organizacji OWASP
- SQLMap – skrypt Python do wyszukiwania podatności SQL Injection
- Dodatki do przeglądarek, np. Tamper Dev (dodatek do przeglądarki Chrome umożliwiający zmianę parametrów przesyłanych żądań)
- Nessus – automatyczny skaner podatności (aplikacje i serwery)

Testy bezpieczeństwa cd.

Wyniki

Wybrane podatności:

- Broken Access Control (błędne zarządzanie uprawnieniami)
- Cross Site Scripting (osadzanie skryptów)
- SQL Injection (wstrzyknięcia kodu)

Skutki ?

Operacyjne Centrum Bezpieczeństwa

SOC (ang. security operations center)

Zespół odpowiedzialny za monitorowanie, analizę i reagowanie na zagrożenia bezpieczeństwa informatycznego w organizacji. SOC zbiera, analizuje oraz reaguje na incydenty związane z cyberbezpieczeństwem, działając w czasie rzeczywistym w celu zapewnienia ochrony przed atakami i minimalizacji skutków ewentualnych incydentów.

Środowisko działania zespołu SOC: system SIEM, firewalle, systemy antywirusowe, narzędzia zarządzania incydentami, automatyzacja, dobre praktyki i procedury.

Kompleksowe podejście do bezpieczeństwa informatycznego, pozwalają zespołowi SOC na identyfikowanie, analizowanie i reagowanie na zagrożenia w środowisku.

Więcej informacji: stat.gov.pl/wrota-statystyki

Dziękuję za uwagę!

Marcin Piekarek
e-mail: M.Piekarek@stat.gov.pl

Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego