Ministerstwo Cyfryzacji

Program Współpracy w Cyberbezpieczeństwie – PWCyber *Cybersecurity Cooperation Program*

Public-Private Partnership for the National Cybersecurity System

Robert Kośla, Lt.Col. (Ret.)
Director
Department of Cybersecurity

2020-05-21 – CyberGov 2020 Conference

Cooperation with the industry in cybersecurity…?

Legal background - KSC Law

http://orka.sejm.gov.pl/opinie8.nsf/nazwa/2505_u/$file/2505_u.pdf

DZIENNIK USTAW

RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 13 sierpnia 2018 r.

Poz. 1560

USTAWA

z dnia 5 lipca 2018 r.

o krajowym systemie cyberbezpieczeństwa[1), 2)]

LAW
of 5 July 2018
on a National Cybersecurity System

Legal background - KSC Law

http://orka.sejm.gov.pl/opinie8.nsf/nazwa/2505_u/$file/2505_u.pdf

Chapter 9
Tasks of the minister responsible for digitization

Art. 45. 1 The minister in charge of digitization is responsible for:

1) monitoring the implementation of the Cybersecurity Strategy of the Republic of Poland The Polish National Strategy, hereinafter referred to as "the Strategy", and the implementation of action plans for its implementation;
2) recommending areas of cooperation with the private sector in order to increase of the cybersecurity of the Republic of Poland;
3) the preparation of annual reports concerning:
   a) serious incidents reported by key service providers which affect the continuity of their key services in the Republic of Poland and the continuity of key services provided in Member States of the European Union,
   b) significant incidents reported by digital service providers, including incidents involving two or more Member States of the European Union;
4) carrying out information activities on good practices, programmes educational, awareness-raising and building campaigns and training cyber security awareness, including safe use from the Internet by different categories of users;

Legal background - National Cybersecurity Strategy and its objectives

http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

MONITOR POLSKI

DZIENNIK URZĘDOWY RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 30 października 2019 r.

Poz. 1037

UCHWAŁA NR 125
RADY MINISTRÓW

z dnia 22 października 2019 r.

w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024

RESOLUTION NO 125
COUNCIL OF MINISTERS

of 22 October 2019

on the Cybersecurity Strategy of the Republic of Poland for 2019-2024

4.2 Main objective

Increasing resistance to cyber threats and information protection in the public, military and private sectors and the promotion of knowledge and good practice enabling citizens to better protect their information.

4.3 Specific objectives

Specific objective 1. Develop a national cyber security system.

Specific objective 2. Improve the resilience of administration information systems the public and private sector and the achievement of the capacity to be effective to prevent and respond to incidents.

Specific objective 3. Strengthening national security capacity in cyberspace.

Specific objective 4. Building social awareness and competences in the field of cyber security.

Specific objective 5. building a strong international position of the Republic of Poland in cybersecurity area.

Legal background - National Cybersecurity Strategy and its objectives

http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Monitor Polski – 2 – Poz. 1037

Załącznik do uchwały nr 125 Rady Ministrów z dnia 22 października 2019 r. (poz. 1037)

Strategia Cyberbezpieczeństwa

Rzeczypospolitej Polskiej

na lata 2019–2024

Ministerstwo Cyfryzacji

7.2 A focus on developing cooperation between the public and private sectors

Ensuring security in cyberspace requires a joint effort by the private, public and citizens. The government will continue to build an effective system of public-private partnerships based on trust and shared responsibility for cybersecurity.

At the same time, the public administration will improve its capacity to initiate and run cybersecurity projects. The government will also actively engage in existing and emerging forms of European public-private cooperation and thus promote Polish business internationally.

In order to pursue a new vision of the country's development and support the innovativeness of the Polish economy, it will be important to build a support system for research and development projects in the field of cybersecurity, carried out in cooperation between the scientific world and commercial enterprises.

PWCyber Program - Assumptions

PWCyber – Basic Assumptions

1. Voluntary and active participation in the Programme – non-binding nature
2. Format of partnership
3. No financial commitments
4. Confidentiality clause for designated information (NDA)
5. Possibility of other entities to join - with the agreement of both parties

PWCyber – Trust and Security

The PWCyber Programe, due to the need to build trusted relationships with technology partners, is open to companies originating/based in countries with established formal relationship between the national security authorities with Poland:

- European Union,
- The North Atlantic Treaty Organisation
- NATO partner countries

In the current phase of the program development, the participation of non-EU, NATO and NATO partner countries is not foreseen

The accession of companies to the PWCyber Program requires the identification of government resources to actively implement cooperation within the Program

Past practice has shown that it takes approximately six months to agree on the scope and plan of joint activities under the PWCyber before signing the Agreement

PWCyber Program Architecture

Areas of PWCyber cooperation - as an inspiration rather than a closed list

1. Enhancing public administration competences in the field of cybersecurity
2. Exchange of information on cyber threats
3. Preparing recommendations on cybersecurity
4. Preparation and conduct of cybersecurity assessment and certification
5. Disseminating information on innovations in cybersecurity

1. Enhancing public administration competences in the field of cybersecurity

Improving competences of National Cybersecurity System actors in terms of threat awareness, methods of attacks in cyberspace and legal, organizational and technical skills to counter threats in ICT systems and networks. Actions in this area may include in particular:

- sharing and developing training materials (including multimedia) and information on training paths to improve the skills of users and staff responsible for cybersecurity in the use of the products and services offered
- organization of trainings and workshops events, among other things, to present methods of using security functions, including mechanisms that improve resistance to cyber attacks and increase the level of information protection
- conducting awareness-raising campaigns, organizing competitions on best practices in the use of products and services that enhance cyber security

2. Exchange of information on cyber threats

- Identification of vulnerabilities and risks
- Exchange of information and development of methods for reporting and handling incidents
- Organisation and participation in the exercises

3. Cybersecurity recommendations

Preparation of recommendations in the field:

- configuration of devices and services
- software security desing
- service integration

in a way that maximises the effectiveness of Security Baselines

4. Cybersecurity Assessment and Certification

- Development of new test methods
- Preparation of new evaluation criteria
- Participation and promotion of cybersecurity certification of products and services

5. Promoting information on innovations in cybersecurity

- Promoting innovative solutions and projects in the field of cyber security

- Building partnerships with National Cybersecurity System stakeholders interested in developing, testing and implementing new solutions

PWCyber Program Implementation…

Government Security Program – example of cooperation with Microsoft

Microsoft | Security Engineering Security Development Lifecycle Operational Security Assurance Secure DevOps Open Source Software More All Microsoft Search Cart Sign in

Government Security Program

Microsoft recognizes that people will only use technology they trust, and we strive to demonstrate our commitment to building this trust through transparency and confidential security information. This program is offered to qualified governments to participate.

Overview

The Microsoft Government Security Program (GSP) builds trust through transparency. The GSP provides participants with the confidential security information and resources they need to trust Microsoft's products and services. GSP participants currently include over 45 countries and international organizations represented by more than 90 agencies. Participation enables controlled access to source code, exchange of threat and vulnerability information, engaging on technical content about Microsoft's products and services and access to five globally-distributed Transparency Centers.

Online Source Offering

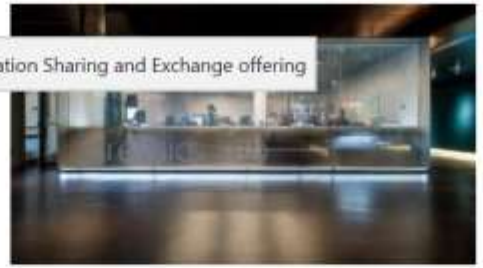
The Online Source offering enables online access to view source code. Microsoft provides access through a secure web portal that provides select source code in a read-only format to Microsoft products such as Windows, Office, SharePoint Server, and Exchange Server.

Learn more >

Transparency Center Offering

Transparency Centers (TCs) are a vital component of the Government Security Program. TCs provide participating agencies with an opportunity to visit a controlled and secure facility to conduct deep levels of source code inspection and analysis. TCs are also an excellent showcase to demonstrate Microsoft's commitment to security and transparency. Visits can be offered at any of the five Microsoft locations around the world that host these facilities.

Learn more >



Information Sharing and Exchange Offering

The Information Sharing and Exchange offering provides data about threats and vulnerabilities and a communication channel with Microsoft security and response teams.

Learn more >

Technical Data Offering

The Technical Data offering provides access to information about products and services. This includes technical documentation about Microsoft's products and cloud services, opportunities to access Microsoft engineers to address specific topics, and security-specific technical trips to Microsoft facilities for deeper face-to-face conversations.

Learn more >

First MoU within PWCyber - Samsung

https://www.gov.pl/web/cyfryzacja/ministerstwo-cyfryzacji-i-samsung-podpisaly-porozumienie-na-rzecz-cyberbezpieczenstwa

Ministry of Digitization

About the ministry | What we do | News | Settle the matter | Contact | PL

Ministry of Digitization > News > Messages > The Ministry of Digitization and Samsung have signed an agreement on cyber security

Return

The Ministry of Digitization and Samsung have signed an agreement on cyber security

02.10.2019

Government plenipotentiary for cybersecurity, minister Karol Okoński and president of Samsung Electronics Polska, Joseph Kim, have signed an agreement today, the purpose of which is to join the Korean company to the Cybersecurity Cooperation Program. The program is implemented by MC in the formula of partnership with the private sector to increase cybersecurity of the Republic of Poland.

5G context in PWCyber – Cisco, Ericsson and Nokia

https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo--kolejne-firmy-z-porozumieniem

Ministry of Digitization

About the ministry What we do

Ministry of Digitization > News > Messages > Cybersecurity - further companies with agreement

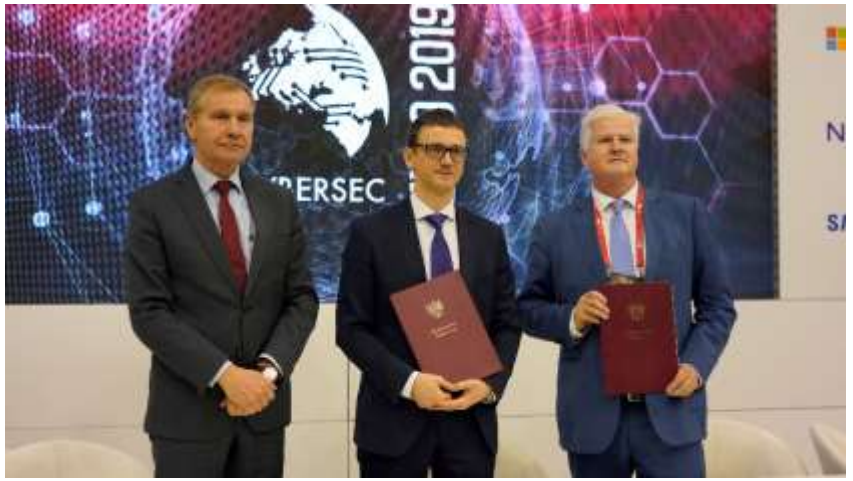
< Return

Cybersecurity - further companies with agreement

10/30/2019

More technology companies are joining the Ministry of Digitization in cyber security.

Three more companies signed an agreement on this matter. It's Cisco, Ericsson and Nokia. The document was signed during the European Cybersecurity Forum CYBERSEC, which took place in Katowice on October 29 and 30, 2019.



Example – PWCyber Implementation Plan with Cisco

Porozumienie Ministerstwo Cyfryzacji Cisco NASK PWCYBER Punkt Porozumienia	Zakres	Działanie	Osoba kontaktowa MC	Osoba kontaktowa Cisco	Status Jan 23 2020
I.2.1) a)	Udostępnianie materiałów szkoleniowych (w tym multimedialnych) oraz informacji o ścieżkach szkoleniowych podnoszących kwalifikacje użytkowników i personelu odpowiadającego za cyberbezpieczeństwo w zakresie korzystania z oferowanych produktów i usług,	Wykorzystanie Akademi Cisco. Podnoszenie swiadomosc: Introduction I Essentials Budowanie kwalifikacji zawodowych CCNA Operationa &Security Spiecie i integracja z platforma GOV.pl Jezyk Polski Lista akademii udostepniona na GOV.pl	Monika Pieniek	Anna Czacharowska	Pani Monika spina procesy. Technicznie jest to wspierane przez NASK. Docelowo wsparcie ze strony COI. Punkty po spotkaniu Ania & Monika - MC robi pilotaż wewnątrz ministerstwa, żeby wyłapac problemy - MC zastanowi się nad dostosowaniem treści - na ww potrzeby uruchomione zostanie konto akademii dla Min Cyfr na netacad.com (ryzyko długotrwałej procedury po stronie MC) - za ok 6 miesięcy (czerwiec) integracja z zewnętrznymi platformami (Single Sign On) być moze będze to wystarczająco dobre rozwiązanie kwestii autentykacji uzytkowników gov.pl - konkurs omówione o możliwosci i dobrych praktykach ze strony Cisco . Na tą chwilę jest to kwestia drugorzędna w stosunku do ww. (wazne ale nie pilne) Ważne i pilne do zrobienia MC procesuje zgloszenie do programu NETACAD po swojej stronie, akceptację umow itp, żeby wystarowac z pilotem, jendoczesnie analizuje tresci i zastanawia sie nad dostosowaniem zagadanień prawnych do warunków polskich.
I.2.1) b)	Organizację wydarzeń szkoleniowych i warsztatowych m.in. celem prezentacji metod korzystania z funkcji zabezpieczających, w tym mechanizmów podnoszących odporność na cyberataki oraz zwiększających poziom ochrony informacji	**Cisco Engage** Cykliczna Konferencje IT zawierajaca komponent Cyberbezpieczenstwa **Umieścic w kalendarzu wydarzen na gov.pl**	Monika Pieniek	Agnieszka Goralowska	Przekazac kalendarz wydarzen do umieszczenia na Gov.pl
		Cykliczne warsztaty dla administratorów Dedykowane do konkretnych technologii w obszarze cyberbezpieczeństwa. **Umieścic w kalendarzu wydarzen na gov.pl**	Monika Pieniek	Agnieszka Goralowska	Przekazac kalendarz wydarzen do umieszczenia na Gov.pl
		Wskazać podmiotom podlegającym Ustawa o KSC, gdzie i w jaki sposób mogą szukać u partnerów porozumienia wsparcia w			Przekazać do wykorzystania dokumenty: Przykładowo Analiza narzedzi dla MyTree atack które mogą pomoc w

Polish Crypto Company in PWCyber – Krypton Polska

https://www.gov.pl/web/cyfryzacja/pierwsza-polska-firma-przystapila-do-programu-wspolpracy-w-cyberbezpieczenstwie-pwcyber

Ministry of Digitization

About the ministry | What we do | **News** | Settle the matter

Ministry of Digitization > News > Messages > The first Polish company joined the Cybersecurity Cooperation Program (PWCyber)

< Return

The first Polish company joined the Cybersecurity Cooperation Program (PWCyber)

10/12/2019

Krypton Polska Sp. z o. o. is the first Polish company to join the Cybersecurity Cooperation Program. On December 10, an agreement on this matter was signed by the government plenipotentiary for cybersecurity, deputy minister of digitization - Karol Okoński and president Michał Czmoch.

AI in Cyberbecurity within PWCyber - IBM

https://www.gov.pl/web/cyfryzacja/minister-cyfryzacji-we-wroclawiu-cyberbezpieczenstwo-i-nowe-technologie-w-sztuce

Ministerstwo Cyfryzacji

O ministerstwie | Co robimy | **Aktualności** | Załatw sprawę

Ministerstwo Cyfryzacji > Aktualności > Wiadomości > Minister cyfryzacji we Wrocławiu: cyberbezpieczeństwo i nowe technologie w sztuce

< Powrót

Minister cyfryzacji we Wrocławiu: cyberbezpieczeństwo i nowe technologie w sztuce

27.01.2020

IBM to kolejna firma, która dołącza do naszego Programy Współpracy w Cyberbezpieczeństwie.

European cryptography and OT in PWCyber - THALES

https://www.gov.pl/web/cyfryzacja/prezydent-francji-w-polsce-wspolpraca-w-obszarze-cyberbezpieczenstwa-priorytetem

Ministry of Digitization

About the ministry | What we do | **News** | Settle the matter

Ministry of Digitization > News > Messages > The President of France in Poland: cooperation in the field of cyber security is a priority

< Return

The President of France in Poland: cooperation in the field of cyber security is a priority

02/03/2020

The declaration to strengthen Polish-French cooperation in the field of cybersecurity and the agreement on the accession of Thales to the Cybersecurity Cooperation Program (PWCyber) - these are documents that were signed during the Monday visit of the French president to Poland.

- In the face of global challenges related to cybersecurity, and above all to ensure an effective response, we need extensive international cooperation. Poland and France share similar views on this subject. We confirmed this today by signing a Declaration to strengthen cooperation in this area - said Minister of Digitization Marek Zagórski.

Agreement between the Ministry of Digitization and Thales about its accession to the Cyber Security Cooperation Program (PWCyber). The agreement was signed by the Minister of Digital Affairs Marek Zagórski and Herve Multon - Executive Vice President of Thales for Europe and International Organizations.

Polish OT company in PWCyber - Dynacon

https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo-kolejna-polska-firma-przystapila-do-naszego-programu

Ministry of Digitization

About the ministry What we do

Ministry of Digitization > News > Messages > Cyber security: another Polish company has joined our program

< Return

Cyber security: another Polish company has joined our program

19/02/2020

Dynacon Sp. z o. o. is another Polish company with which we will cooperate in the field of cyber security. On Wednesday, the minister of digitization and the company's president signed an agreement on this matter.

The cooperation agreement - together with the minister of digitization - was signed by the president of the company Andrzej Cieślak.

- We expect that our participation in the Program will enable intensification of activities on certification schemes that enable the assessment and confirmation of the level of cybersecurity of technological processes in critical and key infrastructures and services, in particular in the energy, fuel and chemical sectors - said the head of Dynacon Sp. z o. o

Global ICT vendor in Poland joins PWCyber - DELL

https://www.gov.pl/web/cyfryzacja/dell-polska-dolacza-do-programu-pwcyber

Ministry of Digitization

About the ministry What we do

Ministry of Digitization > News > Messages > Dell Polska joins the PWCyber program

< Return

Dell Polska joins the PWCyber program

09/03/2020

The ninth agreement under the Cybersecurity Cooperation Program initiated by the MC (PWCyber) signed! On Monday, DELL Technologies Polska joined us.

- It's an important agreement. DELL is one of the giants of the global market for modern technological solutions. What's more, it is also a firm firmly rooted in Poland, as evidenced even by its factory in Łódź - said Minister of Digital Affairs Marek Zagórski during the signing ceremony. And this one took place at the DELL factory in Łódź.

And …

- Further partners in the negotiations to join the PWCyber
  - Akamai
  - Amazon Web Services
  - FireEye
  - Fundacja Bezpieczna Cyberprzestrzeń (Cyberspace Foundation) - PL
  - HakingDebt - PL
  - Media (MediaRevovery) -PL
  - Oracle
  - PaloAlto
  - Smartech
  - Trend Micro
  - VS Data - PL

PWCyber during COVID-19

Support for remote Public Administration – Home Office:

- Cisco
- Microsoft
- Dell/VMWare

Support for Education – Distant Learning

- Cisco
- IBM
- Microsoft

Thank you for your attention

Robert Kosla
robert.kosla@mc.gov.pl
sekretariat.dc@mc.gov.pl
Twitter: @robertkosla