CYBER TRUST Kongres cyberbezpieczeństwa 28-29/11/ 2023

Cybersecurity Trends and Threats Impacting Poland Today

Ray Sylvain, MSCS, CISA, MBA

Centrum Innowacji i Biznesu Politechniki Wrocławskiej

Politechnika Wrocławska

ISSA POLSKA

Ray Sylvain | smartech^IT Chief Information Security Officer

About Ray Sylvain

With a wealth of cybersecurity and systems architecture expertise, Ray Sylvain is the driving force behind SmarTech-IT's success as the Chief Information Security Officer.

Certified Information Systems Auditor (CISA)

- Security, Compliance, and Identity Fundamentals,
- Cybersecurity Architect Expert
- Azure Security Engineer Associate

University of Miami Cybersecurity Training

MSc. Cyber Security Operations & Leadership

MBA Finance

U.S. Marine Veteran

Ray Sylvain | smartech^IT Chief Information Security Officer

- Ray has a remarkable 13-year military background as a U.S. Marine, where he played a pivotal role in cyber security support for the Department of Defense (DoD).
- As Program Director for the U.S. Air Force, Ray showcased exceptional leadership skills in overseeing enterprise-level solutions.
- With over 20 years of experience as a Systems Analyst, Ray's acute problem-solving abilities ensure SmarTech-IT stays at the forefront of cutting-edge technology.
- Notably, Ray led a team with 90+ years of combined experience in cyber security, systems architecture, and supply chain management, further cementing his reputation as an industry leader.
- Ray played a crucial role in enhancing the security infrastructure for mission-critical platforms, including Small Unmanned Ground Vehicles, Assault Breacher Vehicles, and Vehicle Automated Diagnostic Systems for the U.S. Marines.
- Ray's expertise extends to supporting the development of the Security Operations Center (SOC) network for all of Poland's Local Governments, further showcasing his commitment to fortifying national cyber defense.
- Under Ray's leadership, SmarTech-IT is poised to revolutionize the European Union's cybersecurity landscape and safeguard businesses and governments against evolving cyber threats, starting with the country of Poland.

Key Cybersecurity Trends in Poland

Rising frequency and sophistication of cyberattacks

Evolving attack vectors

- AI & ML Automation
  - Exploitation of vulnerabilities in Cloud computing
  - Exploitation of vulnerabilities in Cloud computing

Targeted attacks on critical infrastructure

- Energy
- Transportation
- Healthcare

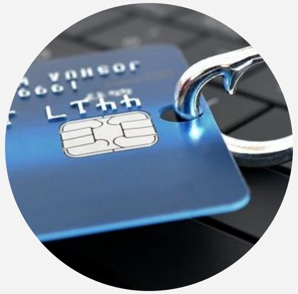
Growing importance of cybersecurity awareness

Increased focus on data protection

- GDPR

Key Cybersecurity Threats Impacting Poland

Ransomware



Phishing

Supply chain attacks

Data breaches

Malware

Some Specific Challenges

- The war in Ukraine
- Poland's growing reliance on technology
- The shortage of cybersecurity professionals

Who Are the Threat Actors (APTs) Attacking Poland?

Russian-backed hacking group **APT28**

Russian-backed hacking group **APT29**

Iranian-backed hacking group **APT35**

North Korean -backed hacking group **APT37**

Chinese-backed hacking group **APT41**

The Latest Major Attacks in Poland (2023)

04.

In April 2023, **APT35** was 🇮🇷 linked to a cyberattack on Polish government websites.

- The attackers defaced the websites with pro-Iranian propaganda.

02.

In February 2023, **APT41** was 🇨🇳 linked to a cyberattack on Polish banks.

- The attackers attempted to steal millions of dollars from bank accounts, but Polish security forces foiled their efforts.

05.

In May 2023, **APT29** was 🇷🇺 linked to a cyberattack on Polish telecommunications companies.

- The attackers attempted to steal sensitive customer data, but Polish security measures blocked their efforts.

03.

In March 2023, **APT37** was 🇰🇵 linked to a cyberattack on Polish power plants.

- The attackers attempted to disrupt the power supply, but their efforts were unsuccessful.

01.

In January 2023, **APT28** was 🇷🇺 linked to a cyberattack on the Polish Ministry of Defense.

- The attackers stole sensitive data, including plans for military exercises and troop movements.

The Latest Major Attacks in Poland (2022)

04.

In April 2022, **APT35** was 🇮🇷 linked to a cyberattack on Polish banks.

- The attackers defaced the websites with pro-Iranian propaganda.

02.

In February 2022, **APT41** was 🇨🇳 linked to a cyberattack on the Polish Ministry of Defense.

- The attackers attempted to steal sensitive military data, but Polish security forces foiled their efforts.

05.

In May 2022, **APT29** was 🇷🇺 linked to a cyberattack on Polish telecommunications companies.

- The attackers attempted to disrupt the country's telecommunications infrastructure, but Polish security measures thwarted their efforts.

03.

In March 2022, **APT37** was 🇰🇵 linked to a cyberattack on the Polish government's email system.

- The attackers stole sensitive government emails, including some related to the country's response to the COVID-19 pandemic.

01.

In January 2022, **APT28** was 🇷🇺 linked to a cyberattack on the Polish Ministry of Foreign Affairs.

- The attackers stole sensitive data, including diplomatic correspondence and intelligence reports.

Recommendations for Mitigating Cybersecurity Risks

01. Developing a cybersecurity strategy:

02. Implementing strong security controls:

03. Raising employee awareness:

04. Adopting a zero-trust approach:

05. Continuous monitoring and improvement:

Recommendations for Mitigating Cybersecurity Risks

01. Developing a cybersecurity strategy:

Organizations need to **develop a cybersecurity strategy** that **identifies their critical assets** and outlines the steps they will take to protect them.

02. Implementing strong security controls:

03. Raising employee awareness:

04. Adopting a zero-trust approach:

05. Continuous monitoring and improvement:

Recommendations for Mitigating Cybersecurity Risks

01. Developing a cybersecurity strategy:

02. Implementing strong security controls:

Organizations need to **implement strong security controls**, such as firewalls, intrusion detection systems, and data encryption.

03. Raising employee awareness:

04. Adopting a zero-trust approach:

05. Continuous monitoring and improvement:

Recommendations for Mitigating Cybersecurity Risks

01. Developing a cybersecurity strategy:

02. Implementing strong security controls:

03. Raising employee awareness:

Organizations need to raise **awareness of cybersecurity risks** among their employees and provide them with **training on how to protect themselves** from cyberattacks.

04. Adopting a zero-trust approach:

05. Continuous monitoring and improvement:

Recommendations for Mitigating Cybersecurity Risks

01. Developing a cybersecurity strategy:

02. Implementing strong security controls:

03. Raising employee awareness:

04. Adopting a zero-trust approach:

Organizations should adopt a zero-trust approach to cybersecurity, which assumes that **no user or device is trusted by default.**

05. Continuous monitoring and improvement:

Recommendations for Mitigating Cybersecurity Risks

01. Developing a cybersecurity strategy:

02. Implementing strong security controls:

03. Raising employee awareness:

04. Adopting a zero-trust approach:

05. Continuous monitoring and improvement:

Organizations need to **monitor** their cybersecurity posture and **make improvements** as needed continuously.

Thank You!

Ray Sylvain, MSCS, CISA, MBA