FAKTORYZACJA CENTRUM BEZPIECZEŃSTWA OPERACYJNEGO

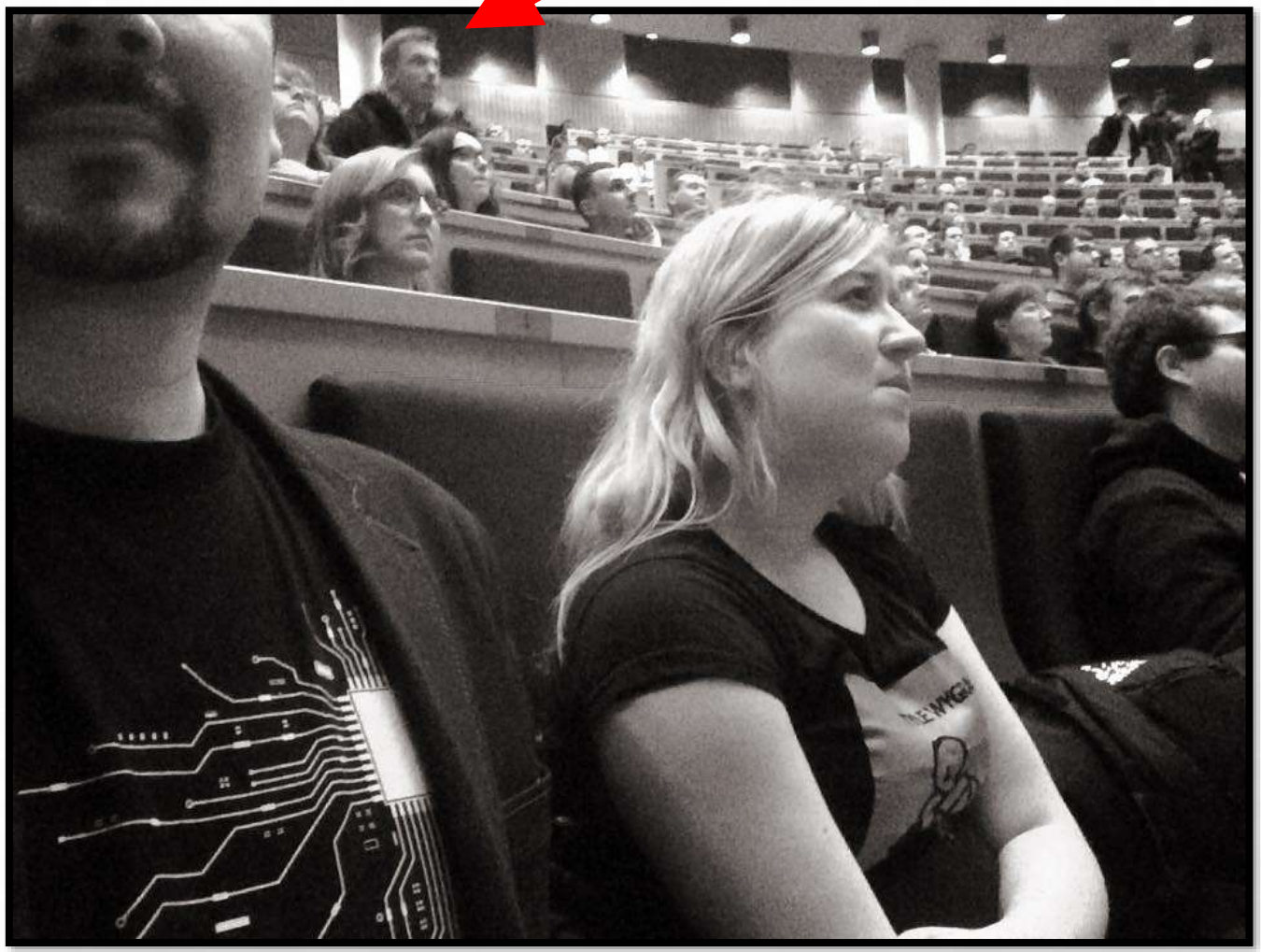
ADRIAN KAPCZYŃSKI

ADRIAN@PTI.KATOWICE.PL

POLSKIE TOWARZYSTWO INFORMATYCZNE

FORMUŁA PRELEKCJI

FORMUŁA PRELEKCJI



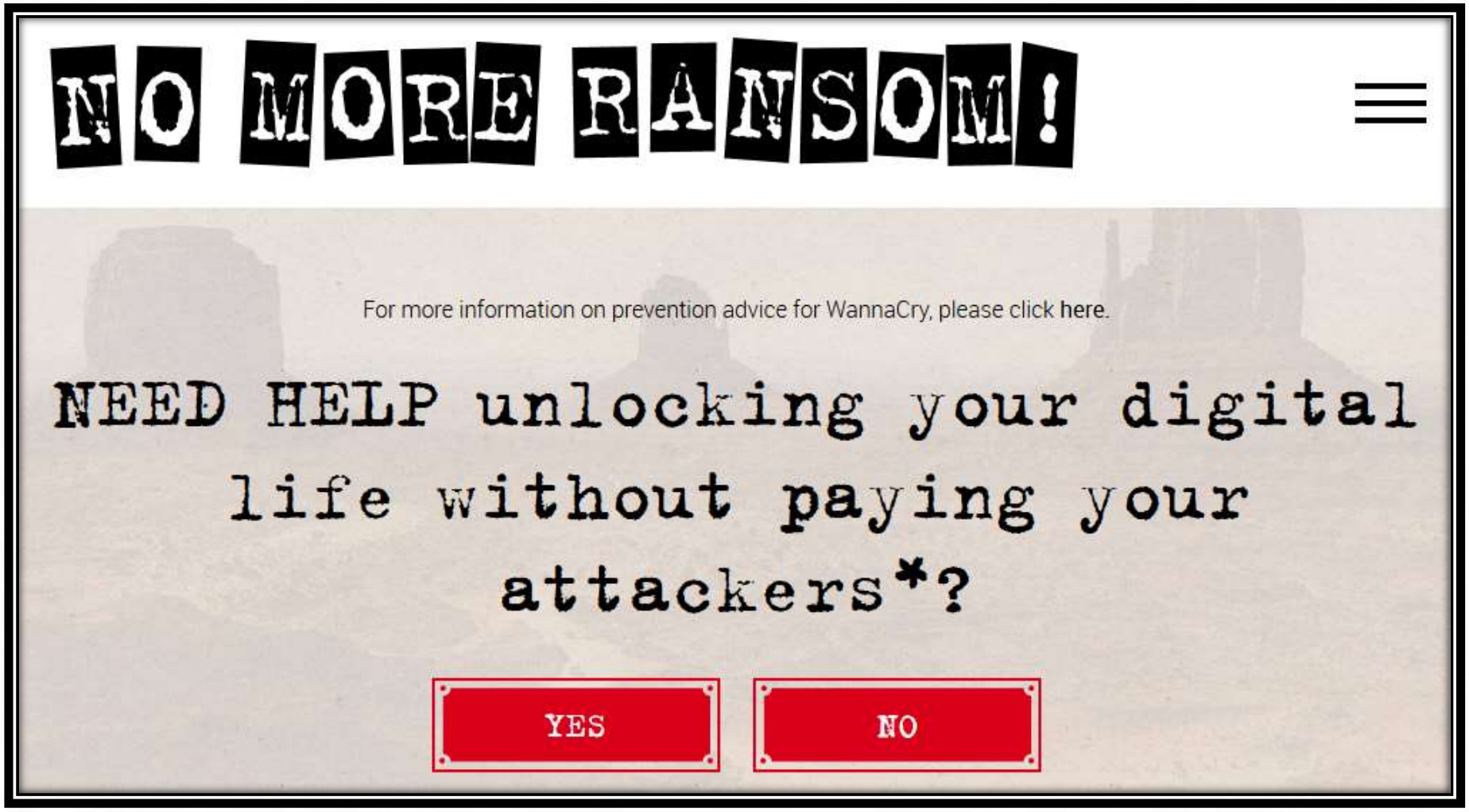
FORMUŁA PRELEKCJI

TYTUŁEM WSTĘPU - TRZY HISTORIE

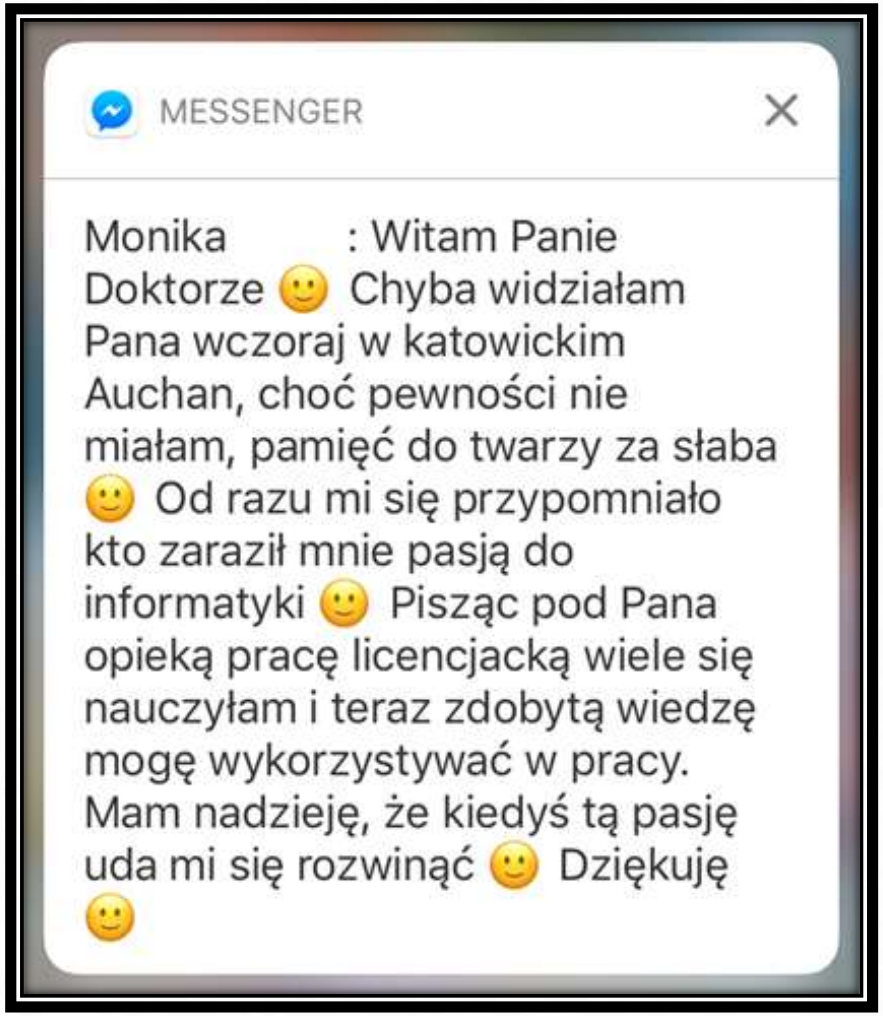
POLSKIE TOWARZYSTWO INFORMATYCZNE (1/2)

Prezesem Oddziału Górnośląskiego PTI (kadencja 2017-2020) został kol. Sławomir Smugowski
(na zdjęciu symboliczne wręczenie prezentu od ustępującego prezesa
oraz pamiątkowe zdjęcie z tortem generalskim)

POLSKIE TOWARZYSTWO INFORMATYCZNE (2/2)



POLITECHNIKA ŚLĄSKA (1/2)



POLITECHNIKA ŚLĄSKA (2/2)

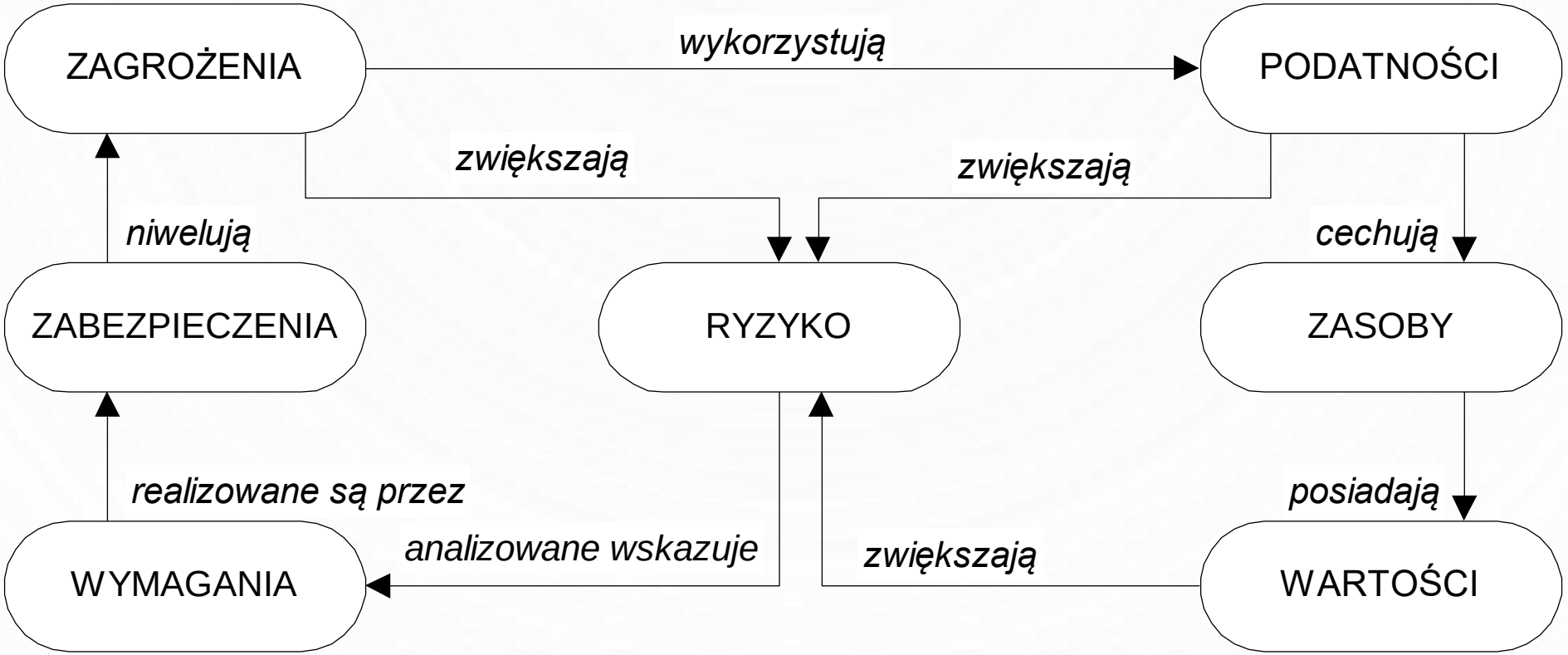
INNE (1/2)

INNE (2/2)

BEZPIECZEŃSTWO TELEINFORMATYCZNE

MODEL, UCZUCIE, RZECZYWISTOŚĆ, OBSERWATOR

MODEL


ZAGROŻENIA
wykorzystują
PODATNOŚCI
zwiększają
zwiększają
niwelują
cechują
ZABEZPIECZENIA
RYZYKO
ZASOBY
realizowane są przez
posiadają
analizowane wskazuje
zwiększają
WYMAGANIA
WARTOŚCI

UCZUCIE

RZECZYWISTOŚĆ

OBSERWATOR

Źródło: http://www.nairaland.com/

CENTRUM BEZPIECZEŃSTWA OPERACYJNEGO

ISTOTNE ZDARZENIA (LOKALNIE)

Podaj istotne zdarzenie związane z bezpieczeństwem informacji, które miało miejsce 2016 roku

0 1 4

- KNF
- yy
- Knf
- Sha1
- Atak na Knf
- Dirty c0w
- Trump
- KNF
- Wybory w USA
- confidence
- Wybory USA
- Ransomware
- Atak na KNF
- Knf

ISTOTNE ZDARZENIA (GLOBALNIE – CZ. 1)

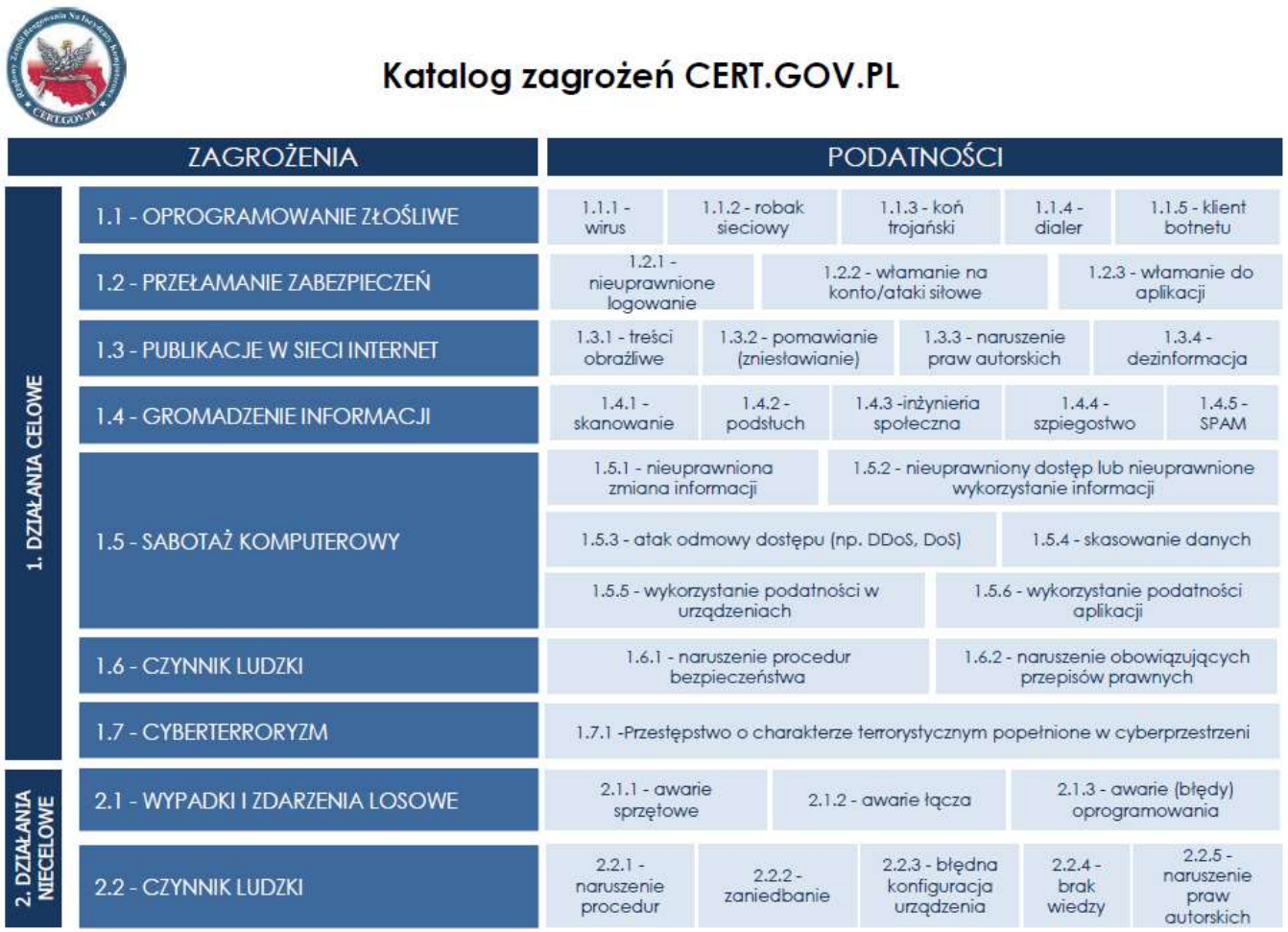
1. Dyn DDoS attack
2. Tesco Bank customers lose real money
3. DDoS automating systems in Finland
4. US Department of Justice employees lose out
5. AdultFriendFinder.com gets attacked once more
6. No 'Peace of Mind' for LinkedIn, Tumblr and Myspace
7. Krebs site hit with DDoS
8. Yahoo suffers from massive data breach #1
9. Yahoo suffers from massive data breach #2
10. Philippine election voters targeted by Anonymous

https://www.welivesecurity.com/2016/12/30/biggest-security-incidents-2016/

ISTOTNE ZDARZENIA (GLOBALNIE – CZ. 2)

1) 4 out of 5 data breaches are attributed to external attacker
2) The majority of data breaches target users and their devices
3) 63% of confirmed data breaches involved weak, default, or stolen passwords
4) In 93% of data breaches, compromise occurred in minutes or less
5) 99% of malware hashes are seen for only 58 seconds or less
6) Just 10 vulnerabilities accounted for 85% of successful exploitations in 2015
7) 50% of attacks happen btw. 10 and 100 days after the vulnerability is published
8) Phishing campaigns have a 30% open rate
9) Email attachments are the #1 delivery vehicle for malware
10) 90% of the data breaches in 2015 followed one of nine common patterns

KATALOG ZAGROŻEŃ I PODATNOŚCI



Katalog zagrożeń CERT.GOV.PL

	ZAGROŻENIA	PODATNOŚCI				
1. DZIAŁANIA CELOWE	1.1 - OPROGRAMOWANIE ZŁOŚLIWE	1.1.1 - wirus	1.1.2 - robak sieciowy	1.1.3 - koń trojański	1.1.4 - dialer	1.1.5 - klient botnetu
	1.2 - PRZEŁAMANIE ZABEZPIECZEŃ	1.2.1 - nieuprawnione logowanie	1.2.2 - włamanie na konto/ataki siłowe	1.2.3 - włamanie do aplikacji		
	1.3 - PUBLIKACJE W SIECI INTERNET	1.3.1 - treści obraźliwe	1.3.2 - pomawianie (zniesławianie)	1.3.3 - naruszenie praw autorskich	1.3.4 - dezinformacja	
	1.4 - GROMADZENIE INFORMACJI	1.4.1 - skanowanie	1.4.2 - podsłuch	1.4.3 -inżynieria społeczna	1.4.4 - szpiegostwo	1.4.5 - SPAM
	1.5 - SABOTAŻ KOMPUTEROWY	1.5.1 - nieuprawniona zmiana informacji	1.5.2 - nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji			
		1.5.3 - atak odmowy dostępu (np. DDoS, DoS)	1.5.4 - skasowanie danych			
		1.5.5 - wykorzystanie podatności w urządzeniach	1.5.6 - wykorzystanie podatności aplikacji			
	1.6 - CZYNNIK LUDZKI	1.6.1 - naruszenie procedur bezpieczeństwa	1.6.2 - naruszenie obowiązujących przepisów prawnych			
	1.7 - CYBERTERRORYZM	1.7.1 -Przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni				
2. DZIAŁANIA NIECELOWE	2.1 - WYPADKI I ZDARZENIA LOSOWE	2.1.1 - awarie sprzętowe	2.1.2 - awarie łącza	2.1.3 - awarie (błędy) oprogramowania		
	2.2 - CZYNNIK LUDZKI	2.2.1 - naruszenie procedur	2.2.2 - zaniedbanie	2.2.3 - błędna konfiguracja urządzenia	2.2.4 - brak wiedzy	2.2.5 - naruszenie praw autorskich

Źródło: http://www.cert.gov.pl/download/3/168/KatalogzagrozenCERTGOVPL.pdf

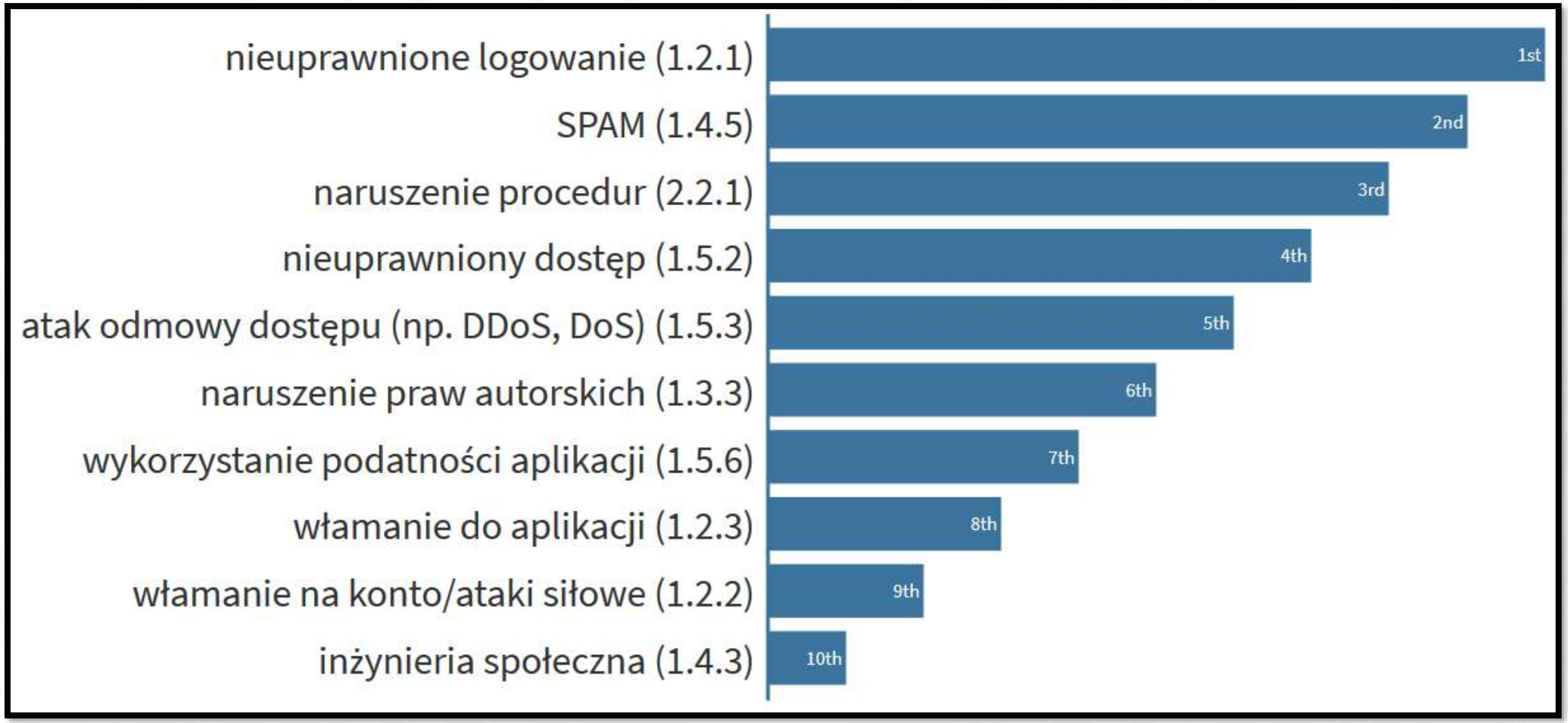
PRIORYTETYZACJA PODATNOŚCI

- … z naszej perspektywy

ZAPRASZAM DO WYRAŻENIA OPINII

ZAPRASZAM DO WYRAŻENIA OPINII

WYNIKI PRIORYTETYZACJI



POKAZ

POKAZ (ŹRÓDŁA) – CZ. 1

- Początki (1999 r.): http://www.systel.pl/oferta/
- Przykład otwierający: https://www.dpd.com/ (podziękowania dla Adama Ziaji (https://adamziaja.com)
- Urządzenia w sieci: https://censys.io/ (alternatywnie: http://shodan.io/)

POKAZ (ŹRÓDŁA) – CZ. 2

- Kamery internetowe: https://www.insecam.org/
- Mysz w sieci: http://dweet.io/
- Pliki w sieci: http://share.pho.to/Ag5WI

POKAZ (ŹRÓDŁA) – CZ. 3

- Zagrożenia (cz. 1): http://cybersquirrel1.com/
- Zagrożenia (cz. 2): http://map.norsecorp.com/#/
- Zagrożenia (cz. 3): http://www.digitalattackmap.com/gallery/
- Zagrożenia (cz. 4): https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
- Zagrożenia (cz. 5): http://www.hackmageddon.com/

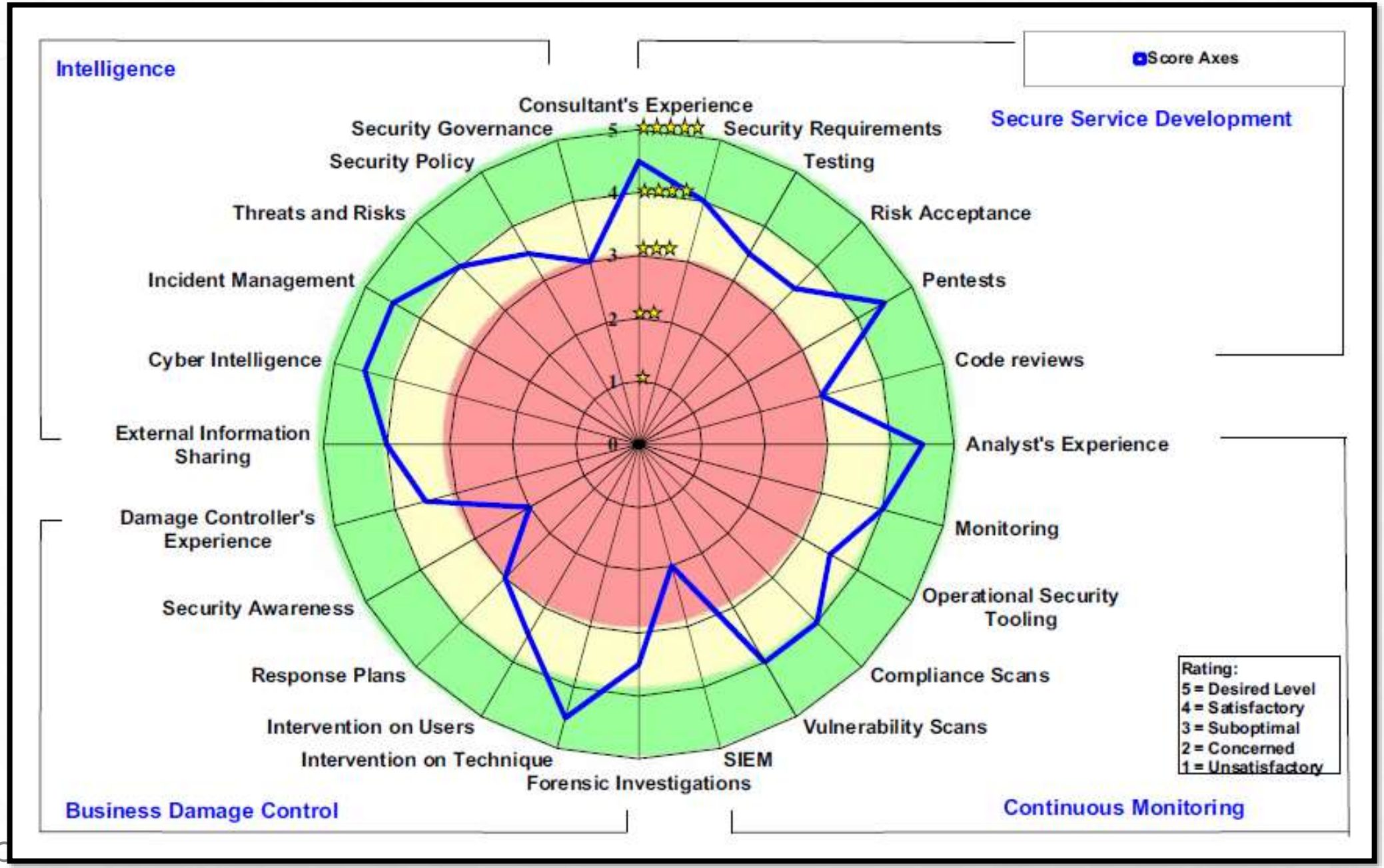
POKAZ (ŹRÓDŁA) – CZ. 4

- Raporty (cz. 1): https://dyzurnet.pl/download/multimedia/raporty/raport_2016.pdf
- Raporty (cz. 2): https://www.cert.pl/PDF/Raport_CP_2016.pdf
- Raporty (cz. 3): https://blog.barkly.com/verizon-2016-dbir-summary-top-10-stats
- Raporty (cz. 4): https://www.thalesgroup.com/sites/default/files/asset/document/2017_thales_data_threat_report.pdf
- Raporty (cz. 5): https://www.sonicwall.com/whitepaper/2017-sonicwall-annual-threat-report8121810/
- Raporty (cz. 6): https://www.symantec.com/security-center/threat-report
- Raporty (cz. 7): https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf

POKAZ (ŹRÓDŁA) – CZ. 5 (DODATKOWA)

- Ciekawa historia: https://exatel.pl/advisory/paranoicy-raport-socexatel.pdf

PODSUMOWANIE



Źródło: http://ieeexplore.ieee.org/document/7070084/?reload=true

CIEKAWE ZASOBY

CIEKAWE ZASOBY

1. http://ieeexplore.ieee.org/document/7070084/?reload=true
2. http://ai2-s2-pdfs.s3.amazonaws.com/f5c6/8f1c3135ace2a71e31070e73453c4f3a190b.pdf
3. http://dimsystem.pl/wp-content/uploads/2017/02/20_Uslugi_budowy_Security_Operation_Center_DimSystem_folder_produktowy_2016.pdf
4. *www.pse.pl/uploads/pliki/9399SIWZ_17092015_2_CZ_II.pdf*
5. https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110011188.pdf
6. http://rafeeqrehman.com/wp-content/uploads/2014/12/Building_SOC.pdf
7. https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907
8. http://iv2-technologies.com/SOCConceptAndImplementation.pdf
9. https://defcon.org/images/defcon-18/dc-18-presentations/Pyorre/DEFCON-18-Pyorre-Building-Security-Operations-Center.pdf
10. http://people.cs.ksu.edu/~xou/publications/siw14.pdf

DZIĘKUJĘ!