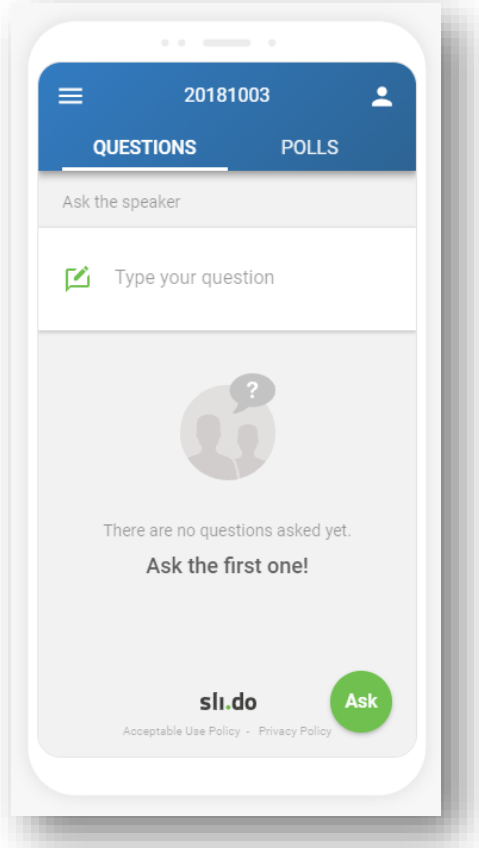
Techniczna strona RODO, czyli kilka słów o wyniku złączenia formalnych oraz nieformalnych źródeł wiedzy Inspektorów Ochrony Danych

Adrian Kapczyński
adrian.kapczynski@pti.org.pl

Polskie Towarzystwo Informatyczne
Sekcja Przyszłości IT

Tytułem wstępu

- slido.com
  - #Konwent

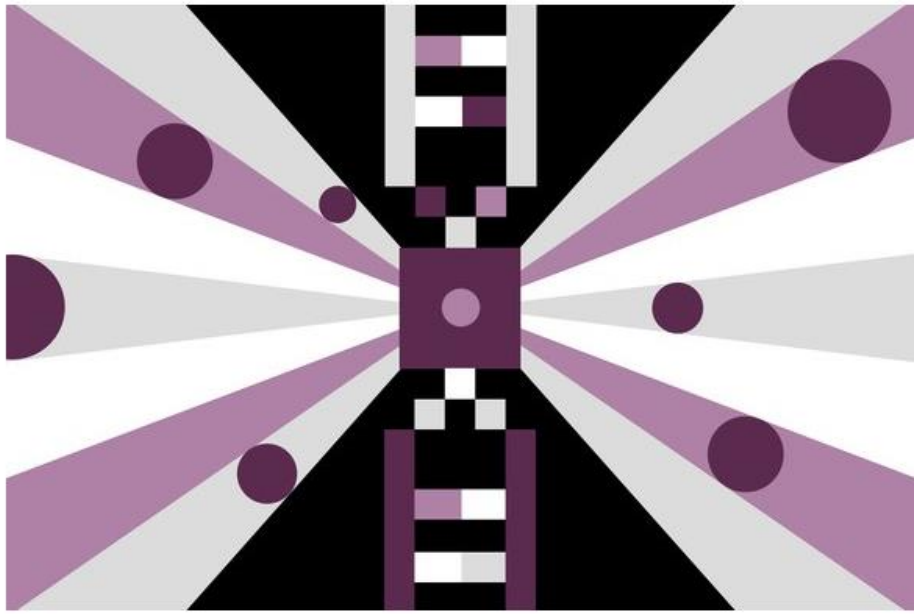


Wprowadzenie

https://tiny.pl/t9n4s

DANIEL OBERHAUS SCIENCE 03.21.19 06:10 PM

FINALLY! A DNA COMPUTER THAT CAN ACTUALLY BE REPROGRAMMED



DNA computers have to date only been able to run one algorithm, but a new design shows how these machines can be made more flexible—and useful. LA TIGRE

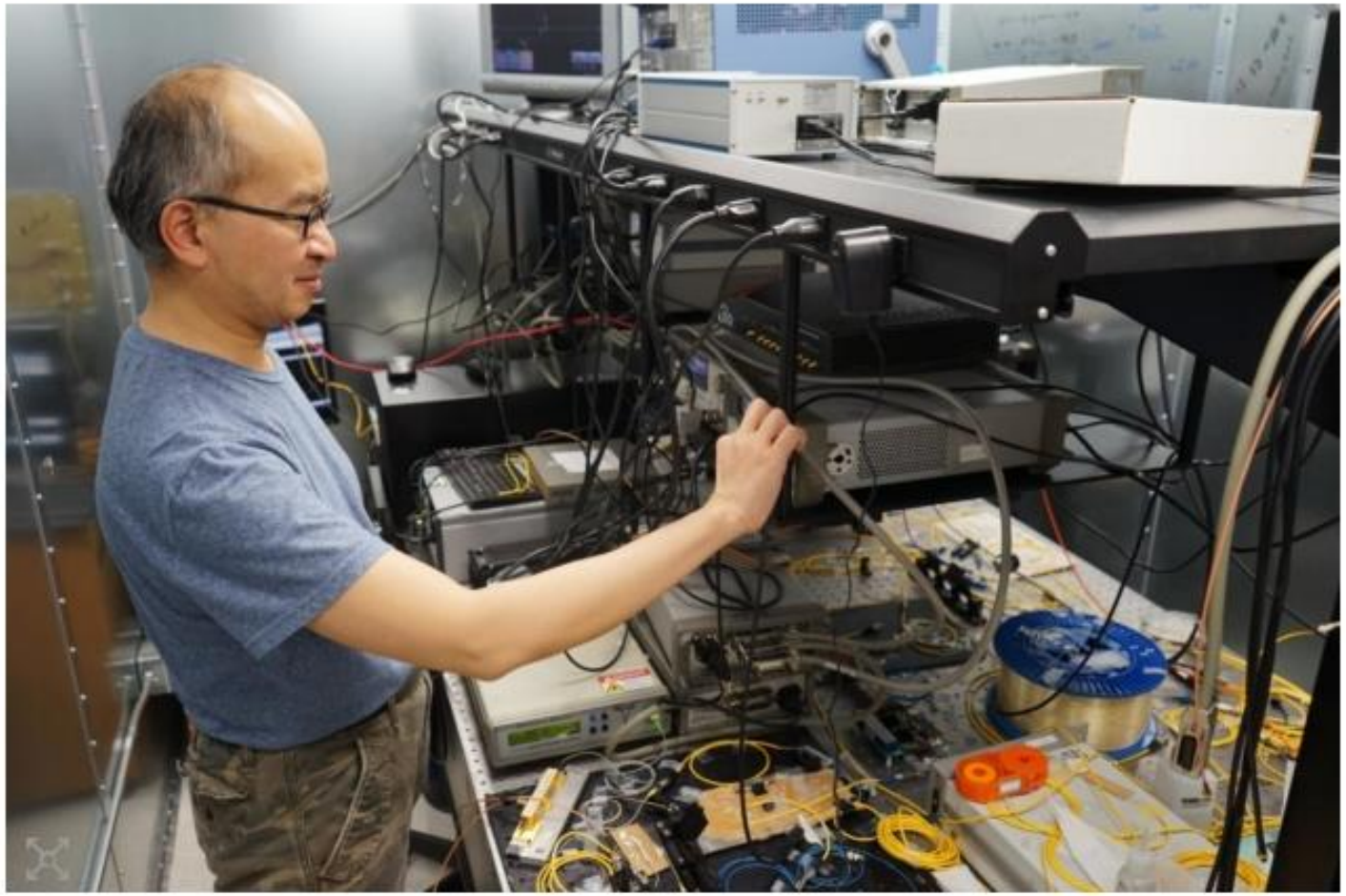
DNA IS SUPPOSED to rescue us from a computing rut. With advances using silicon petering out, DNA-based computers hold the promise of massive parallel computing architectures that are impossible today.

https://tiny.pl/t9nnf

MATERIALS | RESEARCH UPDATE

The quantum internet comes closer

31 Jan 2019 Belle Dumé



Hoi-Kwong Lo (ECE) and his collaborators have performed a proof-of-principle experiment on a key aspect of all-photonic quantum repeaters. (Credit: Jessica MacInnis)

https://tiny.pl/t9nnp

DIGITAL TRANSFORMATION TRENDS 2019

*data taken from Forbes Article "Top 10 Digital Transformation Trends For 2019"

parallel CONSULTING

5G Fixed to 5G Mobile

New companies are paving the way for other 5G providers to start offering new, innovative services for mobile users. There's no doubt that we will start seeing 5G on the top corners of our phone as early as next year.

Blockchain – Hot Tech or Hot Mess?

There will be a lot of wise developers who will continue seeing the full potential of blockchain throughout 2019, but these developers might have to prepare themselves for the waiting-time of deploying such applications on a large scale

3X–4X

More effectively used data with a sound investment in Data, Analytics, Machine Learning & AI digital programmes

GDPR

Misuse of personal data will impact brand identity, marketing and selling – all business-critical initiatives to keep the customer happy and coming back.

It's Still All About That Cloud Connection: Public, Private and Hybrid

NLP & Sentiment Analysis Help Chatbots Find Their Way

The Rise of ITaaS

CEO's To Lead Digital Transformation

Move Aside VR...

AR is the Stronger Reality

Edge and Core Computing Merge With Growth of IoT To Maximise Data Utilisation

https://tiny.pl/t9nn2

https://tiny.pl/t9nkx

Jakość nagrania z monitoringu okazała się zbyt niska.
Sztuczna inteligencja nie pozwoliła na rozpoznanie szczegółów
infografiki na pojeździe, którego kierowca dokonał szkody.

Bezpieczeństwo holistyczne

XXIII Jesienne Spotkania
Polskiego Towarzystwa Informatycznego
Wisła, 16–18 października 2007r.

PTI
Polskie Towarzystwo Informatyczne

Historia spotkań : 2007 : 2008 : 2009 : 2010 : 2011

Czwartek, 17 III 2016 r.

- Aktualności
- Powitanie...
- Propozycje sesji
- Key Notes
- Program ramowy
- Program szczegółowy
  - Sesje plenarne
  - Sesje uczestników
    - Bezpieczeństwo holistyczne...
    - Google Hacking
    - 7 cudów...
    - Dlaczego godzimy się na buble?
    - E-government - szansa czy utopia?
    - Aroganccy indywidualiści
    - E-edukacja, E-nauczyciele...

Bezpieczeństwo holistyczne: ochrona zasobów, cyberśledztwo oraz zapewnienie ciągłości działania

Termin sesji i "lokalizacja":

godzina:	poniedziałek 15 X 2007		wtorek 16 X 2007		środa 17 X 2007		czwartek 18 X 2007		piątek 19 X 2007	
9:00-13:00	W/T 1	W/T 3	SU	SU SU	SU	SU SU	SU	SU SU	W/T 2	W/T 4
			przerwa obiadowa							
14:00-18:30			SP		SP		SP			
20:00-...	IP		IP		IP					

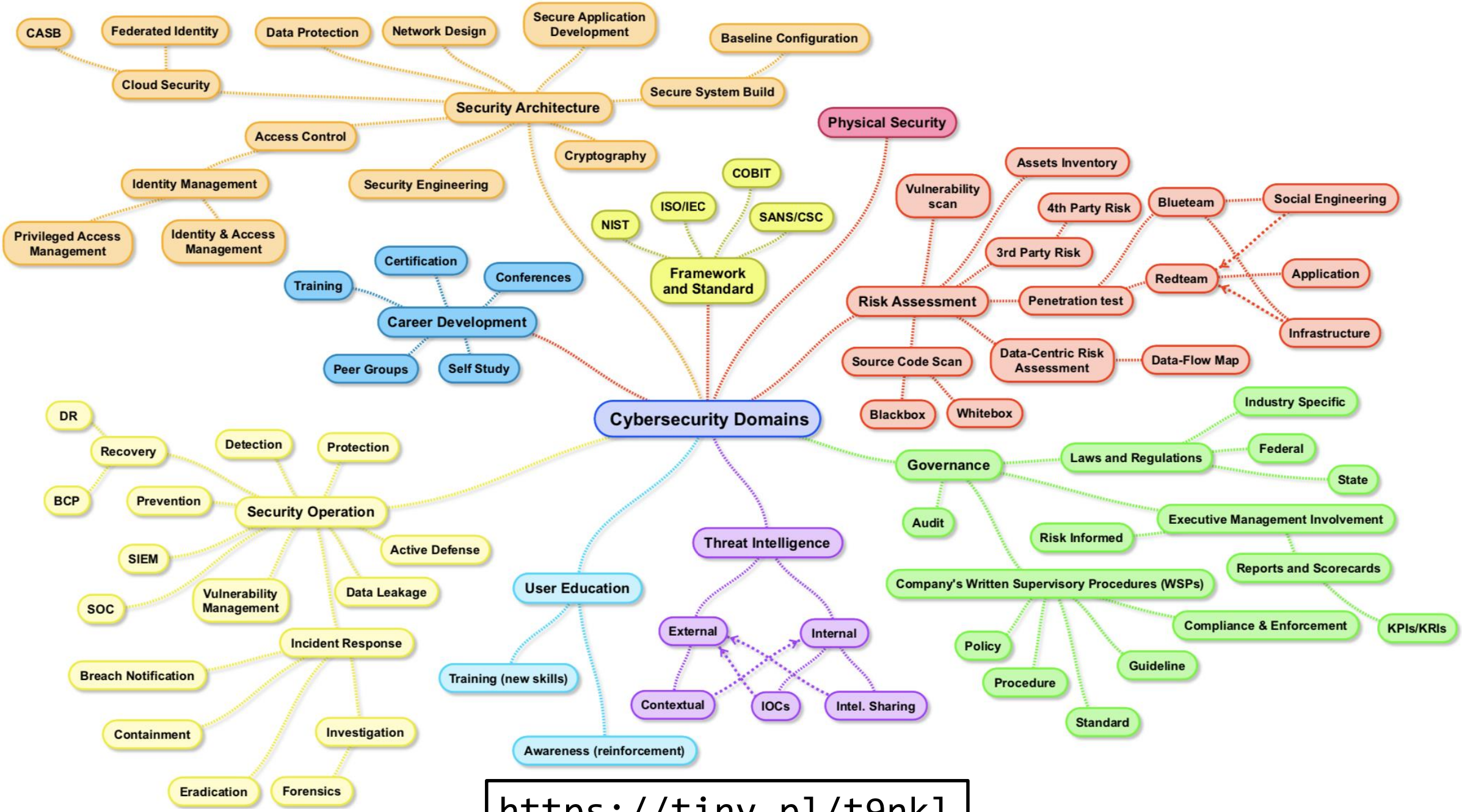
LOGOWANIE:
e-mail:
hasło:
Zaloguj
Zapomniałeś/łaś hasła?
Problemy z logowaniem?

SUBSKRYPCJA:
Newsletter dotyczący konferencji PTI OG:
Zapisz mnie...
Chcę zrezygnować...

Najczęściej czytane:
- Powitanie / Strona główna
- Jak skutecznie prowadzić projekt typu web 2.0?

Kryptowirologia (2007) vs. Oprogramowanie szantażujące (2019)

https://tiny.pl/ttjqx

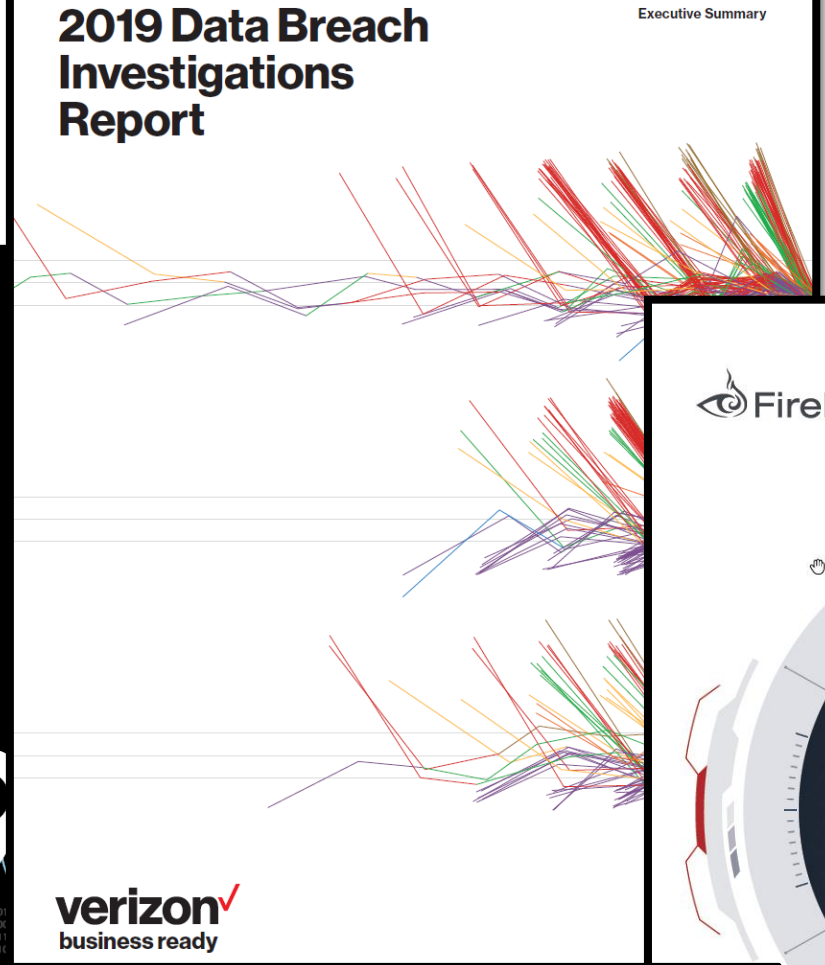


https://tiny.pl/t9nkl

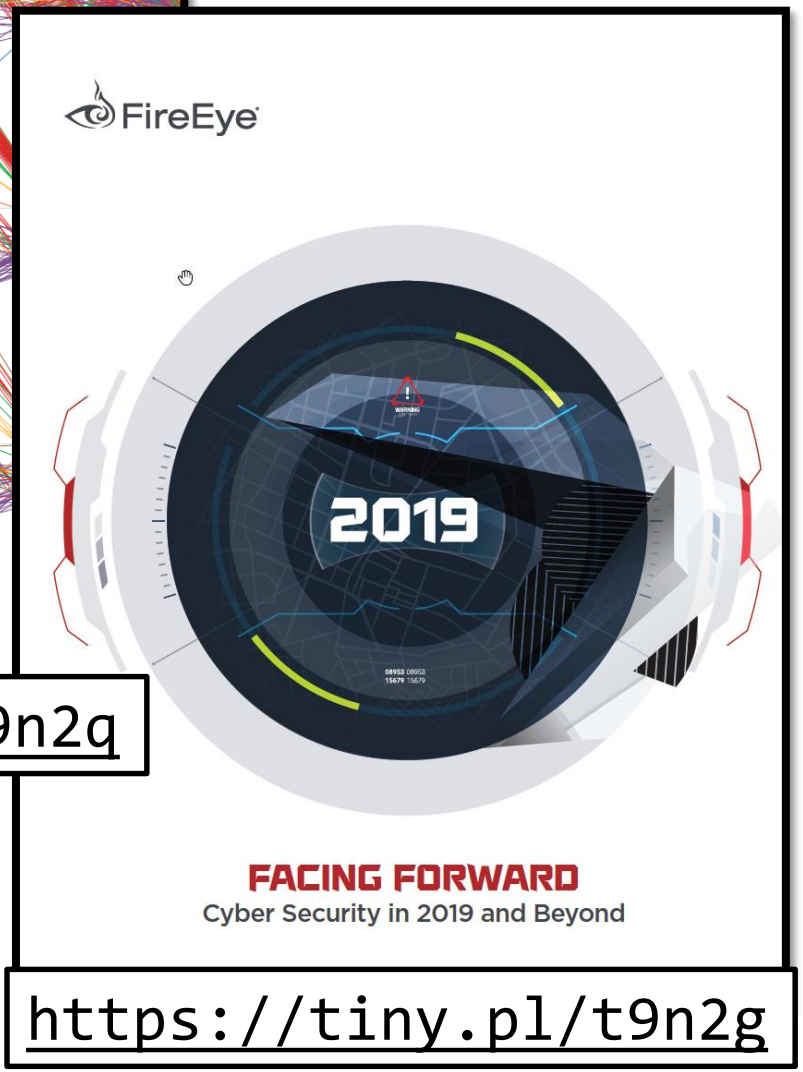
Formalne źródła

https://tiny.pl/t9nk2

https://tiny.pl/t9n6g



https://tiny.pl/t9n2q



https://tiny.pl/t9n2g

01 Attackers will exploit artificial intelligence (AI) systems and use AI to aid assaults

02 Defenders will depend increasingly on AI to counter attacks and identify vulnerabilities

https://tiny.pl/t95jg

:\>TECH INFO\UODO



Irlandzki odpowiednik UODO (DPC) https://www.dataprotection.ie […]13 maja 2019 r. został poinformowany przez WhatsApp Ireland o poważnej luce w zabezpieczeniach platformy. Luka mogła umożliwić zainstalowanie nieautoryzowanego oprogramowania i uzyskać dostęp do danych osobowych na urządzeniach, na których zainstalowano WhatsApp.

https://tiny.pl/t9n2r


PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
dr Edyta Bielak-Jomaa

Warszawa, dnia 15 marca 2019 r.

DECYZJA

ZSPR.421.3.2018

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2018 r. poz. 2096, z późn. zm.) oraz art. 7 ust. 1 i 2, art. 60 i art. 101 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000, z późn. zm.) w związku z art. 12 ust. 1, art. 14 ust. 1 - 3 i art. 58 ust. 2 lit. d i lit. i oraz z art. 83 ust. 5 lit. b rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zmianą ogłoszoną w Dz. Urz. UE L 127 z 23.05.2018, str. 2), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez X. Sp. z o. o., Prezes Urzędu Ochrony Danych Osobowych

aruszenie przez X. Sp. z o. o., przepisów art. 14 ust. 1-3 rozporządzenia
ropejskiego i Rady UE 2016/679 i Rady UE 2016/679 z dnia 27 kwietnia 2016

Nieformalne źródła

Axence Polska
276 obserwujących
7 h

+ Obserwuj

Dziś na PGE Narodowy wydarzenie Axence Partner Day połączone z konferencją prasową i premierą raportu "Władcy Sieci - Wyzwania zarządzania i bezpieczeństwa IT". Zebraliśmy ponad 500 ankiet od administratorów / specjalistów IT aby zobrazować stan polskiego IT, główne zagrożenia i wyzwania oraz codzienne obowiązki problemy informatyków. Wyniki badania zaprezentował **Robert Poslajko** z **Axence Polska**. Na konferencji poprosiliśmy o komentarz ekspertów. W debacie wzięli udział: **dr Maciej Kawecki** z **Ministerstwo Cyfryzacji**, **Michal Jaworski** z **Microsoft**, **Artur Cieslik** z **IT Professional**, **Robert Siudak** z **Instytut Kościuszki** oraz **Grzegorz Oleksy** z **Axence Polska**. W drugiej debacie gościmy reprezentantów firm technologicznych **Bartosz Leoszewski** z **FancyFon Software Ltd**, **Artur Cyganek** z **Acronis** oraz **Magdalena Baraniewska** z **F-Secure Polska**.

Bardzo mocno wybrzmiała konieczność wzmocnienia roli i znaczenia specjalistów IT w organizacjach, znaczenie edukacji użytkowników, powszechność zagrożeń typu wycieki danych - a w konsekwencji niezbędność zaangażowania środków w budowanie zabezpieczeń. Rola informatyków w firmach przeszła z roli "technika" do pozycji mocno osadzonej w biznesie. W wielu [illegible]anizacjach mocno przyczyniło się do tego RODO. [illegible]ny raport na **raport.axence.net**

https://tiny.pl/t9n2d

https://www.facebook.com/groups/forum.abi/

https://tiny.pl/t95jr

UODO nałożył drugą karę na podstawie RODO

autor: **Sławomir Wikariak** 16.05.2019, 17:25; Aktualizacja: 16.05.2019, 17:29

Udostępnij na Facebooku | Udostępnij na Twitterze

RODO. Dane osobowe źródło: ShutterStock

Urząd Ochrony Danych Osobowych nałożył drugą karę na podstawie RODO. Jeden ze związków sportowych bezprawnie udostępniał na swej stronie internetowej szczegółowe dane sędziów, w tym ich adres i PESEL. Kara w wysokości niespełna 56 tys. zł to przede wszystkim jednak wynik tego, że choć związek wiedział o naruszeniu, to przez pół roku nie naprawił swego błędu.

O naruszeniu ochrony danych poinformował prezesa UODO sam związek w lipcu 2018 r. Nie krył tego, że wskutek niezamierzonego działania, na jego stronie internetowej pojawiły się dane 585 osób, którym przyznano licencje sędziowskie. Poza imionami i nazwiskami także takie, których nie było wolno udostępniać – dokładne adresy zamieszkania i numery PESEL. Związek sam też powiadomił o swym błędzie wszystkich zainteresowanych.

https://tiny.pl/t95td

Forum Inspektorów Ochrony Danych | Adrian | Strona główna | Utwórz

Forum Inspektorów Ochrony Danych

Grupa zamknięta

Interakcja jako Ty

- Informacje
- **Dyskusja**
- Ogłoszenia
- Członkowie
- Wydarzenia
- Filmy
- Zdjęcia
- Pliki

Szukaj w tej grupie

PRAWO.GAZETAPRAWNA.PL

RODO nie jest głupie, ale bywa głupio stosowane

Do przepisów o ochronie danych osobowych trzeba podchodzić nie tylko z…

23 33 komentarze

Lubię to! Komentarz

Słowo "głupie" jest nieadekwatne. RODO jest po prostu zle napisane. Jakby pisał je ktoś kto się uczy pisac akty prawne, albo ktoś kto nie zna zasad wykładni, albo jakby ktoś zapomniał gdzie schował ostateczną redakcję tekstu. Koncepcja nie jest zła, re… Zobacz więcej

Lubię to! · Odpowiedz · 2 d · Edytowano 10

A moim zdaniem problem jest gdzie indziej. Zamiast szukać znaczenia w przepisach i ich istocie, pochylamy się nad tym co mówią literki, kropki i przecinki. No i do tego stosowania należy dodać krajowe przepisy - konia z rzędem temu, kto uzasadni po co … Zobacz więcej

Lubię to! · Odpowiedz · 2 d 4

One też się same nie napisały.

Lubię to! · Odpowiedz · 2 d 2

Napisz odpowiedź…

Nie wolno stosować zasad wykładni prawa krajowego do prawa UE. Nie literalnie, nie gramatycznie. Bardziej funkcjonalnie i celowościowo. I jakoś się da to RODO zrozumieć 🙂 TSUE podkreśla od lat wielojezykowość prawa UE i konieczność analizowania aktów w innych językach. Wszak wiśnia i czereśnia to nie w każdym języku to samo 😉

Lubię to! · Odpowiedz · 2 d 4

odpowiedział · 29 odpowiedzi 7 min

Napisz komentarz…

Prywatność · Regulamin · Reklama ·

https://tiny.pl/t95jr

DPIA i ocena ryzyka w ochronie danych

Piotr Wojczys

CISA CICA

https://tiny.pl/t95jr

Proponowany wykaz rodzajów przetwarzania dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych

Rodzaje/kryteria dla operacji przetwarzania, dla których wymagane jest przeprowadzenie oceny	Przykłady operacji/zakresu danych/okoliczności, w których może wystąpić wysokie ryzyko naruszenia dla danego rodzaju operacji przetwarzania	Potencjalne obszary wystąpienia/ istniejące obszary zastosowań
1. Ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych	Profilowanie użytkowników portali społecznościowych i innych aplikacji w celach wysyłania niezamówionej informacji handlowej (spamu).	Media społecznościowe, firmy marketingowe, firmy headhunterskie.
	Profilowania osób bezrobotnych pod kątem dostępu do różnych form pomocy bez ich zgody.	Urzędy pracy w zakresie profilowania osób bezrobotnych.
	Ocena zdolności kredytowej, przy użyciu algorytmów Sztucznej Inteligencji i żądania ujawnienia danych nie mających bezpośredniego związku z oceną zdolności kredytowej.	Banki, inne instytucje finansowe upoważnione do udzielania kredytów, instytucje pożyczkowe w procesie oceny zdolności kredytowej.
	Ocena stylu życia, odżywiania się, jazdy, sposobu spędzania czasu itp. osób fizycznych w celu np. dla - podwyższenia im ceny składki ubezpieczeniowej, na podstawie tej oceny nazywanym ogólnie optymalizacją składki ubezpieczeniowej	Firmy ubezpieczeniowe – oferowanie zniżek związanych ze stylem życia (papierosy, alkohol, sporty ekstremalne, styl jazdy samochodem).
	Profilowanie pośrednie (ocena osoby na podstawie przynależności do określonej grupy).	Firmy ubezpieczeniowe – np. korzystniejsze oferty ubezpieczeniowe, kredytowe dla pracowników określonych grup np. administracji publicznej, nauczycieli.
2. Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki	Systemy monitoringu wykorzystywane do zarządzania ruchem lub przeciwdziałania zagrożeniom/nadużyciom drogowym, umożliwiające szczegółowy nadzór nad każdym kierowcą oraz jego zachowaniem na drodze w szczególności systemy pozwalające na automatyczną identyfikację pojazdów.	Drogi objęte odcinkowym pomiarem prędkości (system gromadzi informacje nie tylko o pojazdach naruszających przepisy, ale o wszystkich pojazdach pojawiających się w kontrolowanym obszarze), odcinki dróg wyposażone w system elektronicznego poboru opłat viaTOLL.

https://tiny.pl/t95jr

Komentarz nt. zmian legislacyjnych dotyczących stosowania RODO w zakresie pisemnych upoważnień do przetwarzania danych osobowych

Opracował: Piotr Wojczys CISA, CICA

Projekt ustawy zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 (ustawa sektorowa) przewiduje wprowadzenie szerokiego, aczkolwiek wybiórczego obowiązku wydawania przez administratora pisemnych upoważnień do przetwarzania danych osobowych. Mechanizm ten jest wskazywany jako zabezpieczenie zapobiegające nadużyciom lub niezgodnemu z prawem dostępowi lub przekazaniu danych.

Upoważnienia nie są w projekcie ustawy sektorowej skojarzone tylko z przetwarzaniem szczególnych kategoriami danych osobowych, występują tam często, jednak wyspowo. Ten "szczególny środek bezpieczeństwa" miałby mieć szerokie zastosowanie, także w odniesieniu do działań wykonywanych na danych w tak „wrażliwych" obszarach jak te regulowane np.:

- ustawą o szczególnych zasadach odbudowy, remontów i rozbiórek obiektów budowlanych zniszczonych lub uszkodzonych w wyniku działania żywiołu,
- ustawą o samorządach zawodowych architektów oraz inżynierów budownictwa,
- ustawą o planowaniu przestrzennym,

itp.

Stosowanie upoważnienia do przetwarzania danych osobowych w formie samoistnego dokumentu, czyli dotychczasowa praktyka oparta na uproszczonej interpretacji art. 39 ust.2 poprzedniej Ustawy o ochronie danych osobowych, nie znajduje odzwierciedlenia w przepisach RODO, co dostrzega coraz szersze grono ekspertów. Nie dziwi więc, że takie działania nie były i zasadniczo nie są stosowane systemowo w ani w innych krajach UE ani w instytucjach unijnych znajdujących się pod bezpośrednim nadzorem Europejskiego Inspektora Ochrony Danych (EDPS). W RODO sformułowanie „z upoważnienia" (org. „under the authority") odnosi się bowiem do ogólnego władztwa

https://tiny.pl/t95jr

WSKAZÓWKI DOTYCZĄCE ZGŁASZANIA NURUSZEŃ OCHRONY DANYCH OSOBOWYCH (v.2)

Opracował: Piotr Wojczys CISA, CICA.

Przykłady zawarte poniżej mają charakter niewyczerpujący. Mają one pomóc w podjęciu decyzji czy w określonych przypadkach naruszenia ochrony danych osobowych należy dokonać odpowiednich zgłoszeń i zawiadomień.

A. Przykłady kwalifikacji naruszeń ochrony danych osobowych i podmiotów które należy poinformować

Pozycje 2-12 opracowano na podstawie publikacji Europejskiego Inspektor Ochrony Danych (EDPS) pt. „ Guidelines on personal data breach notification For the European Union Institutions and Bodies" 21 November 2018.
https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en

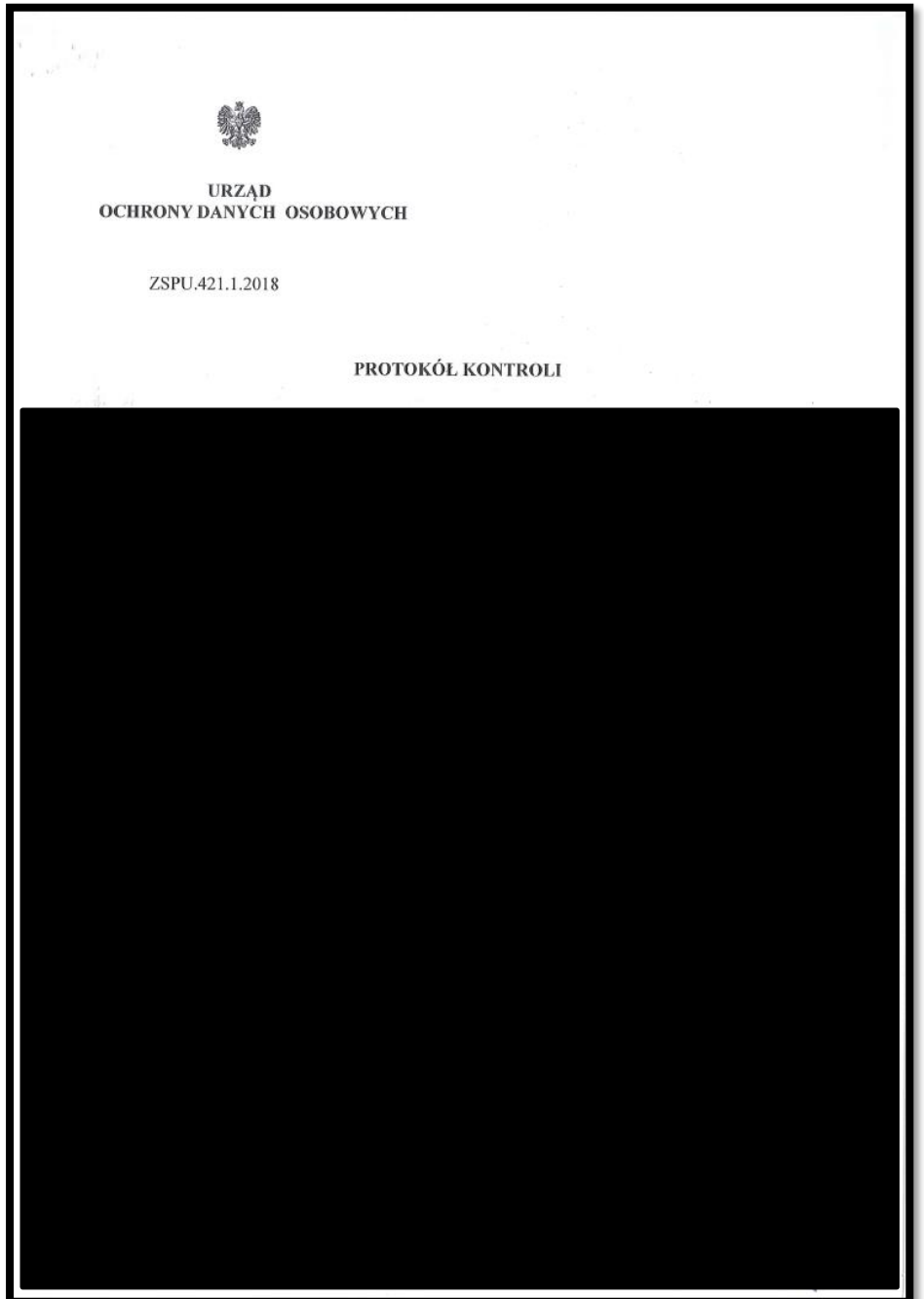
Pozycje 13-16 opracowano na podstawie materiałów opublikowanych przez brytyjski organ ochrony danych – Information Commissioner's Office (ICO) pn. „DPPC 2018:Personal data breach revised case studies".
https://ico.org.uk/for-organisations/resources-and-support/pdb/

Pozycje 17- 26 zaczerpnięto z wytycznych WP250rev.01 Grupy Roboczej Art. 29 (obecnie: Europejska Rada Ochrony Danych) pn. „Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679" Przyjęte w dniu 3 października 2017 r. Ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r.
https://uodo.gov.pl/pl/10/12

Pozycje 1 oraz 26 i następne opracowano na podstawie decyzji wydanych przez Prezesa Urzędu Danych Osobowych.

	Przykład naruszenia	Typ naruszenia	Zgłoszenie organowi nadzorczemu (PUODO)	Zawiadomienie osób, których dane dotyczą o naruszeniu	Wyjaśnienie / Uwagi
1	Dokument urzędowy zawierający imię i nazwisko osoby, jej PESEL oraz zarówno adres zameldowania jak i adres korespondencyjny zostaje omyłkowo wysłany przez ePUAP do innej osoby. Nie ma możliwości wycofania pisma przed jego odbiorem przez niewłaściwego odbiorcę.	Poufność	TAK	TAK	Ponieważ zakres danych osobowych jest szeroki i potencjalnie ułatwia posługiwanie się cudzą tożsamością należy dokonać zgłoszenia i zawiadomienia. Może mieć miejsce np. wykorzystanie numeru PESEL przy głosowaniu w budżecie obywatelskim przez inną osobę i w ten sposób prawa osoby, której dane dotyczą mogą być naruszone.
2	Urząd przenosi się do innego budynku. Pracownicy zewnętrzni zatrudnieni do przeprowadzki znajdują otwartą szafkę z kartotekami kadrowymi i okoliczności wskazują, że brakuje wielu teczek. Teczki zawierają dokumenty z danymi o zdrowiu. Kopie tych danych znajdują się nadal w systemie informatycznym urzędu.	Poufność Integralność	TAK	TAK	Ponieważ teczki zawierają dane szczególnych kategorii, istnieje wysokie ryzyko naruszenia praw i wolności osób.
3	Podmiot leczniczy posiada własną infrastrukturę informatyczną z folderami	Dostępność Poufność	TAK	TAK	Wrażliwy charakter danych (dane szczególnych kategorii) stanowi wysokie

https://tiny.pl/t95jr



URZĄD
OCHRONY DANYCH OSOBOWYCH

ZSPU.421.1.2018

PROTOKÓŁ KONTROLI

[redacted]

https://tiny.pl/t95jr

EKSPERT RODO

OFERTA FAQ HOW-TO O NAS KONTAKT AKTUALNOŚCI

+48 570 996 993 info@ekspertRODO.pl

Skutecznie wspieramy naszych klientów

Business Medyczne Produkcja eCommerce Publiczne Spółki S.A.

https://tiny.pl/t9n8j

Wdrożenia RODO

Szkolenia Podstawowe oraz

NAJNOWSZE ARTYKUŁY

PRZESŁANKI PRZETWARZANIA
RODO W PRAKTYCE

Ale jak to, ja przetwarzam?

20 KWIETNIA 2019

„U licha! już przeszło 40 lat mówię prozą, nic o tym nie wiedząc." mówi znany bohater sztuki Moliera. A ja ostatnio usłyszałem zdanie – „Jeśli cos wpada i nic z tym nie robię, to nie jest przetwarzanie tylko gromadzenie".

PRZESŁANKI PRZETWARZANIA
RODO W PRAKTYCE

Powierzać czy nie powierzać?

9 MARCA 2019

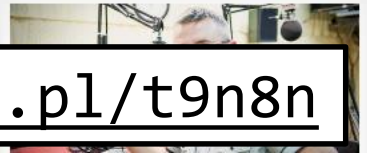
Problem odróżnienia powierzenia od udostępnienia danych chyba nigdy nie zostanie ostatecznie rozwiązany, ale spróbuję się z nim zmierzyć, ku Państwa radości.

ODO W SZKOLE/PRZEDSZKOLU
RODO W PRAKTYCE

Co to są dane osobowe i jak je chronić?

27 LUTEGO 2019

Spory o to, co to są dane osobowe, nie gasną. Spróbuję więc przedstawić moje rozumienie tego zagadnienia oparte o RODO.



CZYTELNIA

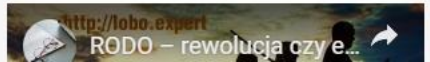
Kącik komputerowy (11)
- Bezpieczeństwo komputerowe (1)
- Bezpieczeństwo sieci (1)
- Szyfrowanie (10)

Prawo autorskie (1)

RODO w praktyce (11)
- Nadużycia i oszustwa (1)
- ODO w szkole/przedszkolu (3)
- Przesłanki przetwarzania (5)
- Szkolenia (1)
- Umowy (2)
- UODO (1)

NA KANALE

Zapraszam do Kącika Inspektora na YT (kliknij ten napis) lub włącz film poniżej:



https://tiny.pl/t9n8n

https://www.facebook.com/groups/3024948836174 95

https://tiny.pl/t9n68

Techniczna strona RODO

Adrian | Strona

Techniczna strona RODO

Grupa otwarta

Interakcja jako Ty

- Informacje
- **Dyskusja**
- Czaty
- Ogłoszenia
- Członkowie
- Wydarzenia
- Zdjęcia
- Pliki

Szukaj w tej grupie

Darek Klimowski udostępnił post.

Założyciel · 3 maja o 15:57

https://tiny.pl/t9n68

16 rozwiązań do zabezpieczenia infrastruktury firmowej

+ powiązania z 20 CIS Controls & Resources (CIS-xx)

1 AV / IS

CIS-8

Antivirus, Internet Security

-monitorowanie plików
-skanowanie w czasie rzeczywistym
-analiza heurystyczna
-wykrywanie wirusów
-usuwanie wirusów
-kwarantanna podejrzanych plików
-analiza sygnaturowa
-analiza cyfrowych odcisków dla plików
-często zawiera skanowanie e-maili (funkcja antyspamu)
-korzysta z agentów

2 NSS

CIS-11,12,14,15

Network Segmentation / Separation

-separacja logiczna
-podział sieci na mniejsze segmenty
-wdrożenie bram pomiędzy sieciami
-wdrożenie stref DMZ
-wdrożenie izolacji serwera od domeny przy użyciu IPSec
-segmentacja pamięci dyskowej (LUN masking)
-wdrożenie rozwiązań CDS (Cross Domain) w oparciu o produkty lub technologie

3 FW / NGFW

CIS-9,11,12,14,15

Firewall/ Next Gen. Firewall

-na styku sieci
-warstwa 2-4, 2-7 (NGFW)
-filtrowanie pakietów
-filtrowanie wg portów
-filtrowanie SPI
-filtrowanie URI -NGFW
-filtrowanie procesów
-filtrowanie sesji
-lub połączenie w/w
-korzysta z reguł dot.: adres IP, port sieci, protokół
-analiza sygnaturowa (NGFW)
-wykrywanie aplikacji (NGFW)
-budowany IPS NGFW)

4 PS

CIS-9,12,14

Proxy server

-na styku sieci
-warstwa 7, 3 (NAT)
-uwierzytelnienie użytkowników
-filtrowanie treści
-filtrowanie URIi
-zapisywanie logów
-cenzurowanie treści
-blokada ruchu niepożądanego
-korzysta z czarnych list URL, DNS,
-korzysta z wyrażeń nieregularnych
-korzysta z reguł
-maskuje oryginalny adres IP (np. NAT)

5 IPS/IDS

CIS-8,9,12,19,20

Intrusion Prevention/Detection System

-na styku sieci lub wewnątrz sieci
-warstwa 2 do 7,
-NIDS, HIDS, NNIDS
-analiza pakietów
-śledzenie pakietów
-dekodowanie protokołów
-analiza heurystyczna
-analiza anomalii
-analiza sygnaturowa
-blokada ruchu niepożądanego
-korzysta z reguł
-korzysta z agentów

6 UTM

CIS-3,5,6,8

Unified Threat Management

-zawiera firewall
-zawiera IDS/IPS
-wbudowany VPN
-wbudowany antywirus
-wbudowany serwer proxy
-kontrola aplikacji
-filtrowanie URIi
-wbudowany WAF

7 DLP

CIS-13,16

Data Leak/Loss Prevention

-wykrywanie danych wrażliwych: osobowe, finansowe, zdrowotne
-kontrola zapisu danych
-analiza ruchu
-analiza treści: w użyciu, w ruchu, archiwalnych
-analiza sygnaturowa
-korzysta z reguł
-korzysta z wyrażeń regularnych
-analiza statystyczna
-analiza słownikowa
-analiza cyfrowych odcisków dla danych

8 SIEM

CIS-6

Security Information & Event Management

-filtrowanie zdarzeń
-zapisywanie logów
-analiza zdarzeń
-generowanie raportów
-zarządzanie logami: z aplikacji, baz danych z urządzeń sieciowych
-korelacja danych
-korzysta z reguł

https://tiny.pl/t9n68

9	10	11	12	13	14	15	16
							
CIS-1,2,7,8,9,18,19	CIS-1,2,3,6	CIS-12,13	CIS-4	CIS-14,16	CIS-12	CIS-12,18	CIS-5
EPP/EDR End Point Protection / Detection & Response	**SA** Security Analytics	**DAM** Database Activity Monitoring	**PAM** Privileged Access Management	**IAM (IdM)** Identity Access Management	**WCF** Web Content Filter	**WAF** Web Application Firewall	**MDM/EMM** Mobile / Enterprise Device Management
-monitorowanie końcówek i zdarzeń sieciowych -zapisywanie logów do centralnej DB -wykrywanie podejrzanej aktywności -wykrywanie rzadkich procesów -wykrywanie nierozpoznanych połączeń sieciowych -korzysta z agentów	-warstwa 2 do 7, -klasyfikacja aplikacji -filtrowanie zdarzeń -zapisywanie logów -analiza zdarzeń -generowanie raportów -zarządzanie logami -analiza behawioralna -korelacja danych -identyfikacja kont współużytkowanych -wykrywanie zagrożeń z wnętrza firmy -wykrywanie kont skompromitowanych -analiza podejrzanego ruchu sieciowego	-monitorowanie aktywności aplikacji -monitorowanie pamięci BD -kontrola kont użytkowników uprzywilejowanych -audytowanie działań administratorów systemów i aplikacji -kontrola uprawnień użytkowników -zapisywanie logów w zewnętrznej BD -analiza behawioralna -integracja z IAM -integracja z SIEM -korzysta z reguł -korzysta z agentów	-kontrola dostępu dla użytkowników -kontrola kont użytkowników uprzywilejowanych -monitorowanie komend na produkcji -kontrola kont współużytkowanych -audytowanie działań administratorów systemów i aplikacji	-kontrola dostępu dla użytkowników -zarządzanie użytkownikami -kontrola dostępu do usług -kontrola zakresu uprawnień (RBAC) dostępowych -kontrola uwierzytelnienia użytkowników (SSO)	-filtrowanie słow kluczowych, kategorii -korzysta z UIRBL, SURBL, czarnych list, URI -korzysta z białych list -filtrowanie treści -filtrowanie URIi -blokada stron ww skompromitowanych	-filtrowanie ruchu z/do aplikacji -monitorowanie ruchu z/do aplikacji -blokowanie ruchu z/do aplikacji -analiza sygnaturowa -korzysta z reguł -blokuje szkodliwe oprogramowanie	-obowiązkowe używanie hasła -zdalna konfiguracja urządzeń mobilnych -szyfrowanie systemu urządzenia -szyfrowanie danych -wykrywanie Jailbreak -wykrywanie malware -zdalne, bezpieczne skasowanie danych -zarządzanie konfiguracją VPN, WiFi -zdalne monitorowanie urządzeń -śledzenie lokalizacji urządzenia -korzysta z agentów

Adnotacje:
1.Wszystkie rozwiązania i urządzenia wymagają odpowiedniej konfiguracji, utrzymania i zarządzania przez wykwalifikowanych inżynierów ds bezpieczeństwa.
2.Większość rozwiązań wymaga posiadania (wykupienia) aktualnych subskrybcji wsparcia (np. sygnatury) u ich dostawców.
3.Niektóre rozwiązania są obowiązkowe (wymagania prawne GDPR, compliance, audyt, ISO 27001) dla określonych branż (finanse, zdrowie) -np. DLP, SA, DAM, PAM, IAM, SIEM.
4.Mocno zalecane dodatkowe uwierzytelnienie administratorów przy wykorzystaniu składników MFA (Multi Factor Authentication).

Linki:
https://phoenixts.com/blog/overview-of-firewall-functionality-and-types/
https://www.cisecurity.org/controls/cis-controls-list/
https://sekurak.pl/wprowadzenie-do-systemow-ids/
https://www.netskope.com/blog/10-essential-dlp-features-demand-casb
t-use-cases-and-benefits-security-analytics-tools
dentity-access-management/
n/windows-firewall/domain-isolation-policy-design

https://tiny.pl/t9n68

Przygotowanie: ISSA Polska
Stan na: 3-05-2019, wersja: 1.3

ISSA POLSKA

Demo

Wyniki interakcji

Aktywne głosowanie

sli.do

0 0 0

Źródło wiedzy (formalne/nieformalne)

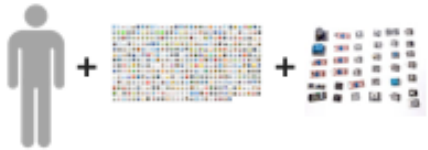
Dołącz na

slido.com

#konwent

Podsumowanie

The Rise of the 4th Platform: A Fabric of Community, Data, Devices, & Intelligence



Billions of Users, Apps, and Sensors

omniconnected fabric of people, intelligence, activity

smart ecosystem **4th Platform**

Sensors (IoT), Machine Intelligence, Mind/Machine UXs

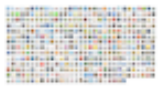
Ambient Computing

effectively infinite network connections

asymptotic network effects

- Dynamic contextual services
- Shared perception & learning
- Ecosystem domination
- Instantly composable apps
- Fully digital business models
- Time augmentation
- Digital communities as institutions

Billions of Users



Millions of Apps

partially connected apps, people, data

ecosystem **3rd Platform**

Web, Social, Mobility, Big Data

Cloud Computing

~one quintillion network connections

high network effects

- Omnichannel user experiences
- Ecosystem competition
- Real-time knowledge flows, economy, and analytics
- App stores, on-demand apps
- Global digital communities
- Hybrid digital business models

Hundreds of Millions of Users

Tens of Thousands of Apps

networking

2nd Platform

Networked PCs, LANs, File Servers, Internet

Distributed Computing

billions of network connections

low network effects

- Sharing & collaboration
- Aggregation of IT
- Productivity
- Decentralization of data capture, storage & computing

Millions of Users

Thousands of Apps

computing

1st Platform

Mainframes, Minicomputers, early PCs

Standalone Computing

0 network connections

no network effects

- Automation
- Efficiency
- Centralization of data capture, storage & computing

https://tiny.pl/t9nsw

Udział w takich wydarzeniach jak

Śląski Konwent Informatyków i Administracji

jest znakomitym sposobem na wymianę informacji pozyskanych zarówno z formalnych, jak i nieformalnych źródeł
(nie tylko na temat technicznej strony RODO)

Do zobaczenia za rok!

Dziękuję!

Adrian Kapczyński
adrian.kapczynski@pti.org.pl

Polskie Towarzystwo Informatyczne
Sekcja Przyszłości IT