



#Cyberbezpieczny(Samo)rząd

Wprowadzenie do szkolenia

Ataki hakerskie na urzędy administracji publicznej
– najczęstsze cyberzagrożenia

Robert Kośla
Dyrektor

Departament Cyberbezpieczeństwa



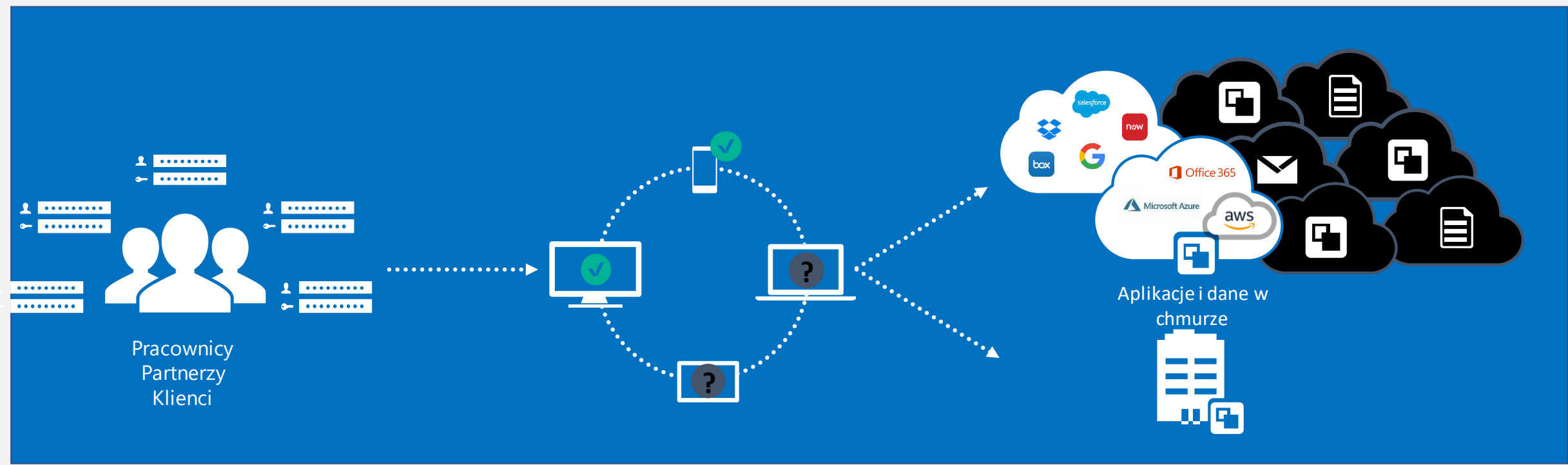


Jakie elementy są aktualnym celem ataków ?

Tożsamość

Urządzenia

Aplikacje i Dane



Mobilność i globalny dostęp

+

Nowe metody ataków

=

Obecne zabezpieczenia nie wystarczają

Ataki na samorządy - przykłady



Polskie Radio 24.pl | Polska | Świat | **Gospodarka** | Sport | Historia | Nauka | Kultura | more_h

Twoje pieniądze | Praca i Firma | Infrastruktura | Rolnictwo | Energetyka

Hakerzy chcą okupu od urzędników z Kościerzyny. Czym jest ransomware?

POLSKIE RADIO 24

Urząd Gminy w Kościerzynie padł ofiarą hakerów. Internetowi przestępcy włamali się na serwery, zablokowali systemy komputerowe oraz dane i zażądali od samorządowców okupu za zdjęcie blokady. Atak spowodował, że mieszkańcy nie mogli uzyskać niektórych usług. Wymaganiem było wypłata w kryptowalucie. Ransomware - stało się popularnym sposobem na wyłudzenie pieniędzy.

TVP 3 ŁÓDŹ | Aktualności | Program TV | Dział Reklamy | Patronaty | Więcej >

dla Ciebie i całej rodziny!

www.toya.net.pl | Infolinia: 42 6333 888

Hakerski atak na Urząd Gminy w Lututowie

2019-12-19 | LUTUTÓW (POW. WIERUSZOWSKI)

NAJNOWSZE INFORMACJE

geoforum.pl

Geodezja | GNSS | GIS | Mapy | Teledetekcja | Narzędzia | Firma | Wojsko | Prawo | Przetargi | Geowiedza | Geodane

PRENUMERATA TRADYCYJNA

PRENUMERATA CYFROWA

Październik 2020 Nr 10 (305)

Przetestuj nasz sprzęt bez wychodzenia z domu! #zostanwdomu YouTube


To już miesiąc paraliżu chełmińskiej geodezji [AKTUALIZACJA]

Od kilku tygodni w PODGiK-u w Chełmnie (woj. kujawsko-pomorskie) geodeci nie są w stanie załatwić żadnej sprawy – zarówno elektronicznie, jak i tradycyjnie na miejscu w urzędzie. Wszystkiemu, jak się okazało, winien

urząd marszałkowski

Urząd marszałkowski w Krakowie sparaliżowany. Hakerzy włamali się na serwery, żądają okupu

05 lutego 2021 | 09:40



NAJCZĘŚCIEJ CZYTANE

- KRAKÓW Spalony budynek archiwum w Krakowie grozi zawaleniem. "Sugestia o tym, że pożar jest miastu na rękę - skandaliczne"
- MATERIAŁ PROMOCYJNY PARTNERA W walentynki zostańcie w łóżku i postawcie na bliskość
- MATERIAŁ PROMOCYJNY PARTNERA Film kontra powieść "Rambo" miał mleć zupełnie inne przesłanie
- KRAKÓW "Sewabska Cyganka" według sądu nie obraża. Sprawa hejtu na Viki Gabor nie trafi na wakacje

SERWIS SAMORZĄDOWY PAP

Prawo | Finanse | Edukacja | Środowisko | Praca | E-urząd | Telekomunikacja | Komitet Regionów | Klub Samorządowy

Małopolski Urząd Marszałkowski zaatakowany przez hakerów

08.02.2021 Aktualizacja: 10.02.2021, 11:48



Najpopularniejsze

- 30 milionów złotych dla JST domów kultury
- Konkursy na dyrektora szkół przesunąć (dokument)
- Ministerstwo edukacji odpuści sprawę zapisów nauczycieli

Ataki w Polsce i na świecie

Atak hakerski na stronę Państwowej Agencji Atomistyki

17 marca 2021, 13:30 ALERT



Na stronie internetowej Państwowej Agencji Atomistyki (PAA) pojawił się komunikat o zagrożeniu radiacyjnym północno-wschodniej Polski. Agencja podała, że był to efekt ataku hakerskiego. Sprawą zajmują się już organy ścigania.

Falszywy alarm

Rano na stronie Państwowej Agencji Atomistyki pojawił się komunikat ostrzegający przed wysokim poziomem promieniowania odnotowanym na obszarze północno-wschodniej Polski. Do uwolnienia radiacji miało dojść na terenie składowiska odpadów promieniotwórczych na Litwie.

Informacja ta jednak została szybko zdemontowana przez PAA w osobnym komunikacie.



WSZYSTKIE TELEFONY 250 ZŁ TANIEJ!

Atak hakerski na MOPS w ... Cyberprzestępcy zażądali okupu


Włamanie, zaszyfrowanie plików i wymuszenie okupu to dosyć popularny sposób działania cyberprzestępców. Przypomnijmy, że pod koniec lutego doszło do hakerskiego ataku na serwer Miejskiego Ośrodka Pomocy Społecznej w ..., co doprowadziło do zaszyfrowania danych na serwerze, obsługującym klientów instytucji. Jednym z celów ataku było wyłudzenie pieniędzy w zamian za odszyfrowanie danych.

24 Andrzej Kozłowski

DOTYCZY: DEZINFORMACJA POLSKI ATOM PAŃSTWOWA AGENCJA ATOMISTYKI NATO OPERACJE INFORMACYJNE MEDIA SPOŁECZNOŚCIOWE

Strona internetowa Państwowej Agencji Atomistyki padła ofiarą cyberataku. Hakerzy umieścili fałszywy komunikat o podwyższonym poziomie radiacji, który następnie został dystrybuowany w mediach społecznościowych. Celem takich działań jest przestrzenie Polaków i ich zniechęcenie do budowy elektrowni atomowej.

ZOBACZ TAKŻE



BEZPIECZEŃSTWO INFORMACYJNE WIRUS, WIRUS WSZĘDZIE! JAK DEZINFORMACYJNE NARRACJE POKAZAŁY NASZE SŁABOŚCI?

Sprawa Microsoftu to sygnał alarmowy: hakerzy mogą zdestabilizować państwo

Grzegorz Kowalczyk
10 marca 2021, 07:40
Ten tekst przeczytasz w mniej niż minutę

Udostępnij na Facebooku Udostępnij na Twitterze



Microsoft / Bloomberg / Kiyoshi Ota

Niespotykana wcześniej skala cyberataku na oprogramowanie Microsoftu pokazuje rosnące możliwości prowadzenia konfliktów w sieci – technologicznych, gospodarczych i politycznych

Ofiarami hakerów padło blisko 30 tys. amerykańskich firm i organizacji, w tym szkoły, instytucje finansowe, nawet agencje rządowe. Atak mógł dotknąć nawet 250 tys. użytkowników. Został przeprowadzony poprzez wejście do Microsoft Exchange – oprogramowania pocztowego dla klientów biznesowych.

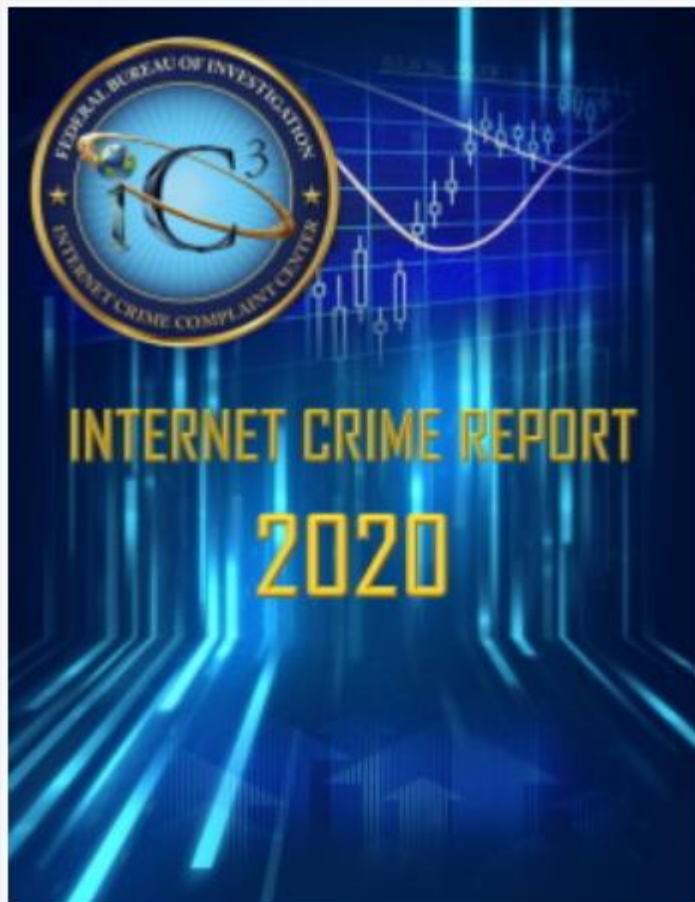
płaci 620 tysięcy za odszyfrowanie plików. Pieniądze wzięto z budżetu drogowego

Strona główna / Aktualności 25.02.2021 16:17





Cyber(nie)bezpieczeństwo kosztuje...



W samych tylko **Stanach Zjednoczonych** cyberprzestępcy w 2020 r. wyrządzili szkody opiewające na **4,2 mld \$**

Koszty cyberprzestępczości z roku na rok wzrastają

Cyberprzestępczość rośnie i chociaż nie powinno to powstrzymywać przed korzystaniem z zasobów online, z pewnością powinno zachęcić **do zwiększenia bezpieczeństwa IT**

Raport: [Internet Crime Report 2020](#)





Cyber(nie)bezpieczeństwo kosztuje...



Raport: [Internet Crime Report 2020](#)

Projekty wspierające bezpieczną informatyzację w samorządach

<https://samorzad.gov.pl/>

gov.pl | Serwis Jednostek Samorządu Terytorialnego | Mój Gov

Koronawirus: aktualne informacje i zalecenia [DOWIEDZ SIĘ WIĘCEJ](#)

Twój samorząd w gov.pl

Uruchom stronę internetową urzędu gminy lub starostwa powiatowego w Serwisie Samorządów Jednostek Terytorialnych na rządowej platformie Gov.pl

DOŁĄCZ

Dołączyli do nas

- Powiat Konecki
- Gmina Zabrodzie

<https://chmura.gov.pl/zuch>

gov.pl | Serwis Rzeczypospolitej Polskiej | Rejestracja

ZUCH^{BETA} System Zapewniania Usług Chmurowych

Usługi Chmurowe

- Bezpieczeństwo**
Zachowanie zasad bezpieczeństwa bez ryzyka dostępu przez niepowołane osoby do danych.
- Optymalizacja kosztów**
Ograniczenie kosztów inwestycyjnych w zakresie infrastruktury i oprogramowania.
- Gotowe rozwiązania informatyczne**
Nielimitowany i zdalny dostęp do danych na każdym urządzeniu z dowolnego miejsca.
- Obsługa urzędu w sytuacji kryzysowej**
Gotowe rozwiązania ułatwiające pracę zdalną, które możesz szybko wykorzystać.



Baza wiedzy o cyberbezpieczeństwie

www.gov.pl/web/baza-wiedzy/aktualnosci

🏠 > Baza wiedzy > Cyberbezpieczeństwo > Dla każdego - cyberhigiena

Aktualności

Dla każdego - cyberhigiena

Dla profesjonalistów

#CyberbezpiecznySamorząd

Szkolenia

Poradniki partnerów technologicznych

Subskrypcje cyberwiadomości

Najczęściej zadawane pytania

Dla każdego - cyberhigiena



Bezpieczni w mediach społecznościowych – poradnik
W poradniku znajdują się wskazówki jak unikać włamań na konta w mediach społecznościowych oraz inne porady dotyczące cyberbezpieczeństwa. (Styczeń 2021 r.)




Media społecznościowe. Jak bezpiecznie z nich korzystać?
Aby zarządzać swoimi cyfrowymi śladami, użyj ustawień prywatności na różnych platformach społecznościowych.




Korzystanie z urządzeń mobilnych
Smartfony, laptopy, tablety – towarzyszą nam dzisiaj praktycznie na każdym kroku. Dlatego warto jest zadbać o bezpieczeństwo danych podczas korzystania z tych urządzeń.

Aktualności


Aktualności



09.03.2021
Dwa składniki, czyli przepis na cyberbezpieczeństwo
Hasła nie są już wystarczającym sposobem na ochronę naszych kont przed przejęciem ich przez cyberprzestępców. Warto stosować dodatkową weryfikację. Oto, o co chodzi i jak to działa.



01.03.2021
Tysiące niebezpiecznych stron
Na liście ostrzeżeń przed niebezpiecznymi stronami jest już ponad 10 tysięcy adresów. Przypominamy, na co zwracać uwagę, by nie stać się ofiarą cyberprzestępców.



01.03.2021
Zapraszamy na kolejne szkolenia online w ramach kampanii #CyberbezpiecznySamorząd!
Nowe tematy bezpłatnych szkoleń z zakresu cyberbezpieczeństwa dla podmiotów publicznych.





Baza wiedzy o cyberbezpieczeństwie



🏠 > Baza wiedzy > Cyberbezpieczeństwo > #CyberbezpiecznySamorząd

Aktualności

Dla każdego - cyberhigiena

Dla profesjonalistów

#CyberbezpiecznySamorząd

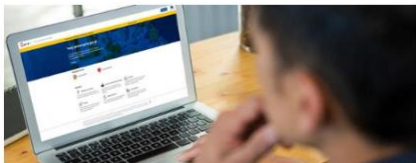
Szkolenia

Poradniki partnerów technologicznych

Subskrypcje cyberwiadomości

Najczęściej zadawane pytania

#CyberbezpiecznySamorząd



Wszystko o portalu samorząd.gov.pl - Poradnik PRCyber - 06

Krok po kroku, jak przystąpić do projektu (Grudzień 2020 r.)



Cyberbezpieczne usługi chmurowe dla administracji publicznej - Poradnik PRCyber-05

Środowisko informatyczne dostarczające usługi chmurowe oraz infrastrukturę IT za pośrednictwem Internetu (Listopad 2020 r.)



Jak sobie radzić ze skutkami ataków typu ransomware? – Poradnik PRCyber-04

Ograniczenie skutków ataków typu ransomware (Sierpień 2020 r.)

Szkolenia

Poradniki partnerów technologicznych

Subskrypcje cyberwiadomości

Najczęściej zadawane pytania

Poradniki partnerów technologicznych

Poradniki partnerów technologicznych



Poradniki

Zapraszamy do zapoznania się z publikacjami partnerów technologicznych.

Rządowe Centrum Legislacji | Polityka cookies | Służba cywilna | Profil zaufany

BIP | Prawa autorskie | Warunki korzystania | Klauzula RODO | Geoportal

Deklaracja dostępności serwisu Gov.pl





Szkolenia dla administracji publicznej



🏠 > Baza wiedzy > Cyberbezpieczeństwo > Szkolenia

Aktualności

Dla każdego - cyberhigiena

Dla profesjonalistów

#CyberbezpiecznySamorząd

Szkolenia


Poradniki partnerów technologicznych

Subskrypcje cyberwiadomości

Najczęściej zadawane pytania


Szkolenia

Harmonogram szkoleń




Informacja o szkoleniach

Zapraszamy na szkolenia dla kadr administracji publicznej organizowane przez Departament Cyberbezpieczeństwa KPRM oraz Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy.



Wracamy ze szkoleniami!

Już 3 lutego ruszają kolejne bezpłatne szkolenia z zakresu cyberbezpieczeństwa – zapraszamy do zapoznania się z nową ofertą i terminarzem szkoleń.



Archiwum szkoleń

<https://www.gov.pl/web/baza-wiedzy/szkolenia>



Ataki hakerskie na urzędy administracji publicznej – najczęstsze cyberzagrożenia



Część 1. Zuzanna Polak

Zgłaszanie incydentów cyberbezpieczeństwa

- zgłaszanie incydentu do CSIRT NASK
- zgłoszenie osoby kontaktowej

Część 2. Kamil Kuć

Omówienie najpopularniejszych cyberzagrożeń

- spam
- phishing
- malware
- ransomware
- kradzież cyfrowej tożsamości





Dziękuję za uwagę

Robert Kośła

robert.kosla@mc.gov.pl

sekretariat.dc@mc.gov.pl

Twitter: @robertkosla

Linkedin: <https://www.linkedin.com/in/robertkosla/>

