Zadanie
„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625

Konferencja naukowa
„Wzmacnianie odporności szkół wyższych
na cyberataki przez podnoszenie kompetencji cyfrowych”

Skuteczne ataki na polskie uniwersytety

Prelegent: dr Krzysztof Świtała
dr Kamil Czaplicki

Ministerstwo Edukacji i Nauki

UKSW Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

CLTC Centrum Liderów Transformacji Cyfrowej

Co to znaczy skuteczny cyberatak?

- Cyberatak (ang. Cyber attack) – atak dokonany za pomocą środków cyfrowych poprzez – cyberprzestrzeń (którego celem są podmioty wykorzystujące cyberprzestrzeń) z zamiarem uszkodzenia, zablokowania dostępu, zniszczenia lub złośliwego przejęcia środowiska obliczeniowego albo naruszenia integralności – danych lub przechwycenia informacji

- Paweł Wiszniewski [w] Wielka Encyklopedia Prawa, tom XXII Prawo Informatyczne, red. Prof. Grażyny Szpor, prof. Lucjana Grochowskiego, wyd. Fundacja „Ubi societas, ibi ius", Warszawa 2021r. s. 88

Skala cyberataków na polskie uniwersytety

Sektor gospodarki	Liczba incydentów	%
Energetyka	4 320	10,89%
Transport	111	0,28%
Bankowość	2 944	7,42%
Infrastruktura rynków finansowych	2 813	7,09%
Służba zdrowia	251	0,63%
Wodociągi	9	0,02%
Infrastruktura cyfrowa	1 821	4,59%
Inne	88	0,22%
Brak	0	0,00%
Administracja publiczna	757	1,91%
Budownictwo i gospodarka nieruchomościami	24	0,06%
Kultura i ochrona dziedzictwa narodowego	30	0,08%
Kultura fizyczna	8	0,02%
Oświata i wychowanie	167	0,42%
Rolnictwo	6	0,02%
Rybołówstwo	1	0,00%
Wyznania religijne i mniejszości narodowe	2	0,01%
Działalność ubezpieczeniowa	35	0,09%
Izby gospodarcze i handlowe	4	0,01%
Handel hurtowy i detaliczny	5 438	13,70%
Produkcja	2 650	6,68%
Logistyka i dystrybucja	15	0,04%
Poczta i usługi kurierskie	6 093	15,35%
Turystyka	10	0,03%
Gospodarka odpadami	3	0,01%
Hotele, restauracje, catering	44	0,11%
Media	7 329	18,47%
Usługi inne	496	1,25%
Osoby fizyczne	4 214	10,62%
TOTAL	39 683	100,00%

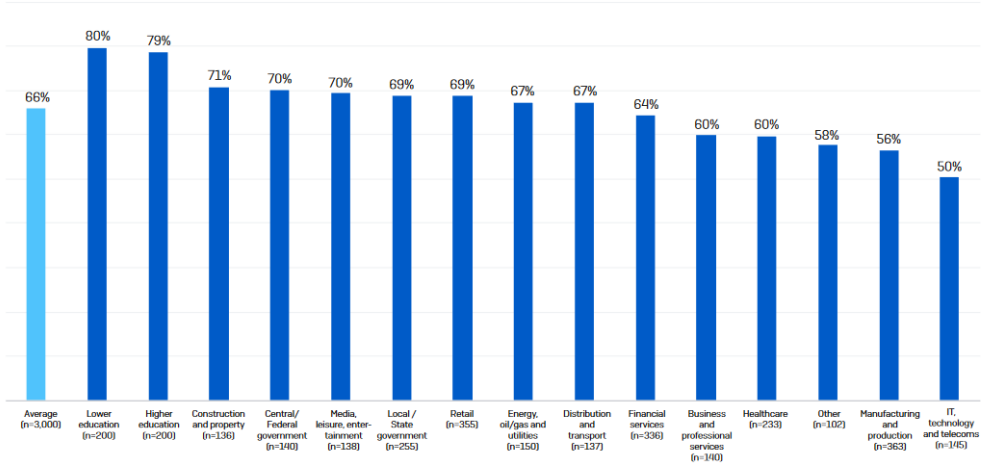
Tab. 1. Incydenty obsłużone przez CERT Polska w 2022 r. w podziale na sektor gospodarki.

Skala cyberataków na polskie uniwersytety

The State of Ransomware 2023

Rate of Ransomware Attacks by Industry

Percentage of Organizations Hit by Ransomware

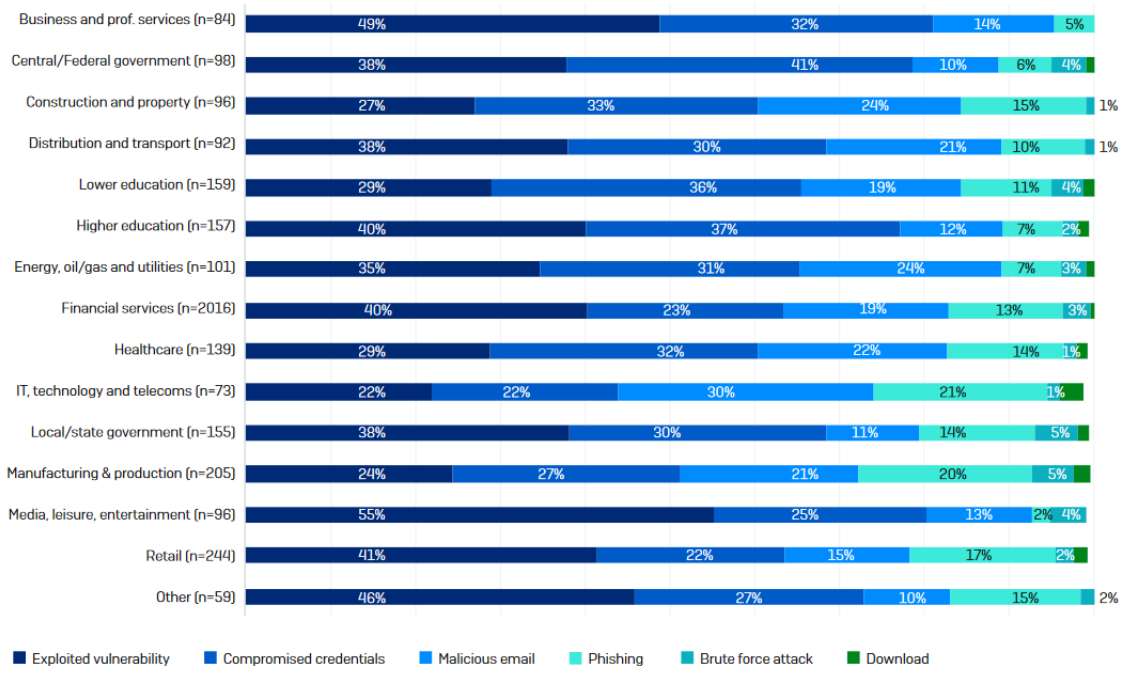


In the last year, has your organization been hit by ransomware? Base numbers in chart

A Sophos Whitepaper. May 2023

The State of Ransomware 2023

Root Cause of Attack by Industry



Do you know the root cause of the ransomware attack your organization experienced in the last year? Selection of answer options. Base numbers in chart

A Sophos Whitepaper. May 2023

Skala cyberataków na polskie uniwersytety

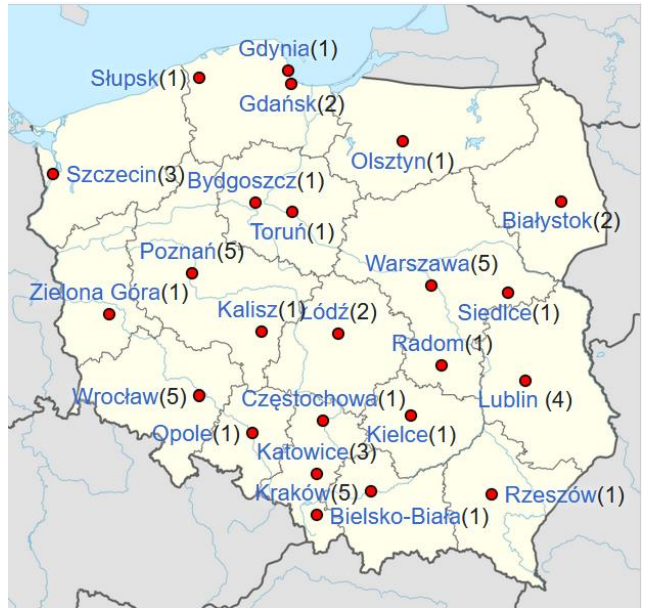
W sierpniu firma Check Point Research opublikowała badania dotyczące **ataków cybernetycznych** na instytucje szkolne i akademickie. Z jej danych wynika, że co tydzień w Polsce dochodzi do przeszło 2700 ataków na szkoły, ośrodki akademickie i badawcze. Podano, że wzrost ataków cybernetycznych na instytucje szkolne i akademickie jest szczególnie widoczny w Polsce.

Ministerstwo Edukacji i Nauki nie odnotowało zgłoszeń czy też skarg dotyczących ataków cybernetycznych na szkoły i uczelnie – poinformowała PAP rzecznik prasowy MEiN Anna Ostrowska

Na przestrzeni ostatniego roku obsłużyliśmy w CERT Polska kilkanaście spraw dotyczących uczelni wyższych lub instytutów badawczych. (...). Natomiast na przestrzeni 3 lat obowiązywania ustawy o krajowym systemie cyberbezpieczeństwa nie jest zauważalny jakiś szczególny trend wynikający z zainteresowania cyberprzestępców akurat tym konkretnym obszarem – przekazał PAP kierownik Zespołu Analiz Bieżących Zagrożeń CERT Polska Sebastian Kondraszuk

https://technologia.dziennik.pl/aktualnosci/artykuly/8232665,cyberatak-polska-uczelnie-pan.html

Kilka przykładów



- Uniwersytet Artystyczny im Magdaleny Abakanowicz w Poznaniu – 22 stycznia 2023r. Atak ransomware
- Uniwersytet Śląski – 22 - 23 lutego 2023r. Atak na wewnętrzną sieć uczelni, poprzez aplikacje myMail
- Poznański Uniwersytet Medyczny- 22 stycznia 2023r. Atak na infrastrukturę IT i wyciek danych pracowników i studentów
- Centralny Szpital Kliniczny Uniwersytetu Medycznego w Łodzi- 6 luty 2023r. Atak ransomware
- SWPS – Uniwersytet Humanistycznospołeczny – maj 2020r.
- Uniwersytet Warszawski- 2020r. Wyciek danych z portalu Wydziału Matematyki, Informatyki i Mechaniki

SGGW – kradzież komputera z danymi kandydatów na studia (11.2019)

Zawiadomienie o naruszeniu ochrony danych osobowych

IOD <iod@sggw.pl>
Do: IOD <iod@sggw.pl>

15 listopada 2019 11:43

Warszawa, dnia 15.11.2019 r.

Szkoła Główna Gospodarstwa Wiejskiego w Warszawie
ul. Nowoursynowska 166
02-787 Warszawa

Szanowna Pani/Szanowny Panie,

Administrator danych osobowych, jakim jest Szkoła Głowna Gospodarstwa Wiejskiego w Warszawie z siedzibą w Warszawie przy ul. Nowoursynowskiej 166, w trybie art. 34 pkt 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO) niniejszym informuje o możliwości naruszenia ochrony Pani/Pana danych osobowych, w związku z incydentem do jakiego doszło w dniu 5 listopada 2019 r. w Warszawie.

W dniu 5 listopada 2019 r. miało miejsce zdarzenie kradzieży komputera przenośnego użytkowanego przez jednego z pracowników Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie. Na dysku tego komputera znajdowały się dane osobowe przetwarzane w trakcie postępowań rekrutacyjnych w ostatnich latach na studia w Szkole Głównej Gospodarstwa Wiejskiego w Warszawie. Administrator Danych Osobowych nie może wykluczyć, iż w wyniku tego incydentu nieznane osoby uzyskały dostęp do Pani/Pana danych osobowych, przez co doszło do naruszenia ochrony danych osobowych. Na dysku komputera znajdowały się dane osobowe kandydatów obejmujące m.in.: dane identyfikacyjne - imię, drugie imię, nazwisko, nazwisko rodowe, imiona rodziców, pesel, płeć, narodowość, obywatelstwo, adres zamieszkania, seria i numer dowodu/paszportu, seria i numer dowodu osobistego, ukończona szkoła średnia, miejscowość szkoły średniej, nr telefonu komórkowego i stacjonarnego, rok ukończenia szkoły średniej, numer i data świadectwa ukończenia szkoły średniej, organ wydający świadectwo, rok matury i data świadectwa maturalnego, organ wydający świadectwo maturalne, wyniki uzyskane na egzaminie maturalnym, ukończone studia, ukończona uczelnia, ukończony kierunek studiów, ocena na dyplomie, średnia ze studiów, kierunek studiów o który kandydat się ubiega, dane szkoły średniej, informacja o zakwalifikowaniu na studia, punkty kwalifikacyjne kandydata, zbieżność kierunku studiów ukończonego z tym o który się kandydat ubiega.

Realizując obowiązek wynikający z treści art. 34 RODO Szkoła Główna Gospodarstwa Wiejskiego w Warszawie informuje, iż istnieje ryzyko nieuprawnionego dostępu do ww. danych osobowych i zapoznania się z ich treścią. Możliwymi konsekwencjami ewentualnego naruszenia ochrony danych osobowych jest nieuprawnione wykorzystanie danych osobowych m.in. w celu:

- uzyskania przez osoby trzecie, na szkodę osoby, której dane naruszono, kredytów w instytucjach pozabankowych, ponieważ wiele takich instytucji umożliwia uzyskanie pożyczki lub kredytu w łatwy i szybki sposób np. przez Internet lub telefonicznie bez konieczności okazywania dokumentu tożsamości;
- uzyskania dostępu do korzystania ze świadczeń opieki zdrowotnej przysługujących osobie, której dane naruszono oraz do jej danych o stanie zdrowia, ponieważ często dostęp do systemów rejestracji pacjenta można uzyskać telefonicznie potwierdzając swoją tożsamość za pomocą numeru PESEL;
- korzystania z praw obywatelskich osoby, której dane naruszono, np.: do głosowania nad środkami budżetu obywatelskiego - uniemożliwiałoby to właściwej osobie skorzystanie z przysługującego jej prawa;
- wyłudzenia ubezpieczenia lub środków z ubezpieczenia, co może spowodować dla osoby, której dane dotyczą, negatywne konsekwencje w postaci problemów związanych z próbą przypisania jej odpowiedzialności za dokonanie takiego czynu.

W celu zabezpieczenia się przed negatywnymi skutkami zaistniałego naruszenia zalecamy, aby osoby których dane osobowe mogły ulec naruszeniu, podjęły kroki minimalizujące ryzyko wystąpienia negatywnych konsekwencji i nieuprawnionego wykorzystania danych m.in. poprzez:

- założenie konta w systemie informacji kredytowej i gospodarczej celem monitorowania swojej aktywności kredytowej (na rynku dostępne są systemy, instytucje i przedsiębiorstwa, które oferują usługi pozwalające na monitorowanie swojej aktywności kredytowej. Podajemy przykładowe: Biuro Informacji Kredytowej S.A. strona https://www.bik.pl, Biuro Informacji Gospodarczej InfoMonitor S.A. strona https://big.pl, Krajowy Rejestr Długów Biuro Informacji Gospodarczej S.A. stron https://krd.pl, Serwis CHRONPESEL strona https://www.chronpesel.pl). W przypadku stwierdzenia jakichkolwiek nieprawidłowości – zgłoszenie tego faktu organom ścigania;
- zachowanie ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu;
- dokonanie samodzielnego zgłoszenia faktu naruszenia danych osobowych właściwym organom w celu zapobieżenia tzw. „kradzieży tożsamości".

Podjęcie tych działań ma na celu zabezpieczenie Pani/Pana danych osobowych przed niewłaściwym ich wykorzystaniem.

Zapewniam, iż Administrator Danych Osobowych w celu zaradzenia naruszeniu ochrony danych osobowych i zminimalizowania ewentualnych negatywnych skutków tego naruszenia podjął niezwłocznie adekwatne środki organizacyjne, administracyjne i prawne, w tym ponownie poinformował pracowników, iż przetwarzanie danych osobowych, których administratorem lub procesorem jest SGGW może odbywać się wyłącznie na nośnikach służbowych zapewniających właściwą ochronę poufności i bezpieczeństwa danych osobowych zgodnie z obowiązującymi w SGGW wewnętrznymi procedurami. Administrator Danych Osobowych przeprowadził też kolejne szkolenie kadry kierowniczej z zakresu przepisów o ochronie danych osobowych oraz kontynuuje harmonogram cyklicznych szkoleń dla pracowników uczelni z tego zakresu. Jednocześnie incydent został zgłoszony przez Administratora Danych Osobowych do Urzędu Ochrony Danych Osobowych i do organów ścigania. Ponadto pracownik Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie będący użytkownikiem skradzionego komputera, złożył zawiadomienie w KP Warszawa Ursynów o podejrzeniu popełnienia przestępstwa przez nieznanych sprawców, polegającego na kradzieży komputera przenośnego zawierającego dane osobowe kandydatów na studia.

Administrator Danych Osobowych, aby zapewnić właściwą ochronę danych osobowych oraz w celu niedopuszczenia do zaistnienia podobnych naruszeń danych, planuje wprowadzenie zmian w sferze stosowanych rozwiązań informatycznych, których celem jest zapewnienie wzmocnionej ochrony danych osobowych. W szczególności, Administrator planuje podjęcie stosownych działań mających na celu ograniczenie możliwości zapisywania danych na nośnikach zewnętrznych.

Administrator Danych Osobowych zapewnia, iż zostały podjęte niezbędne działania, aby podobna sytuacja nie miała miejsca w przyszłości.

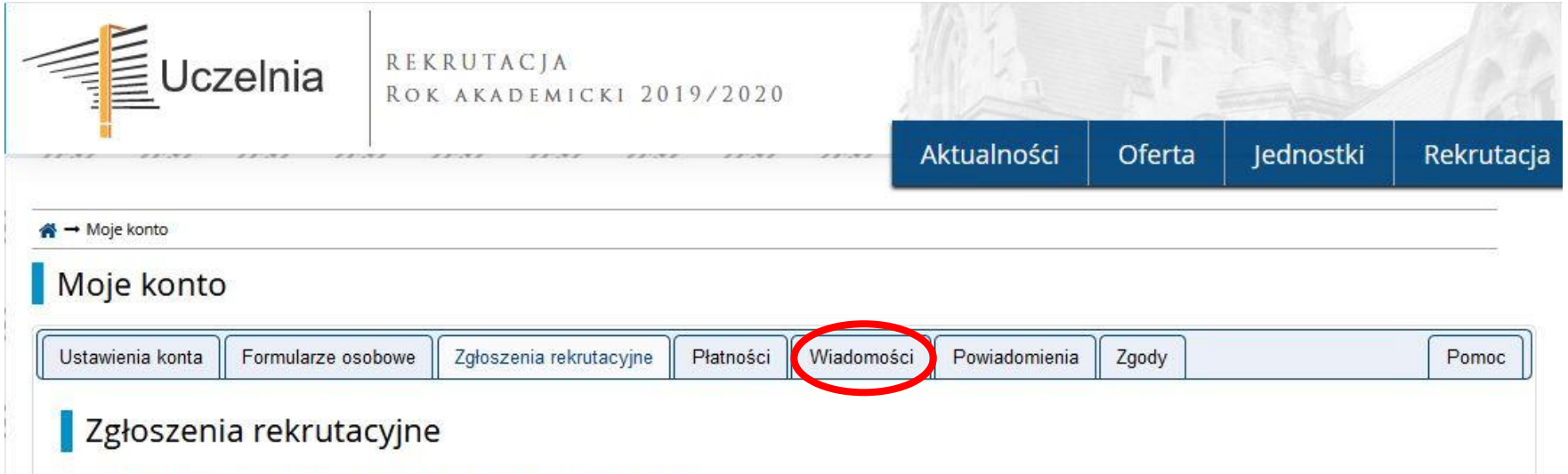
Proza życia – system IRK i jego bolączki mogące doprowadzić do potencjalnych incydentów/naruszeń ochrony danych osobowych

Dzień dobry,

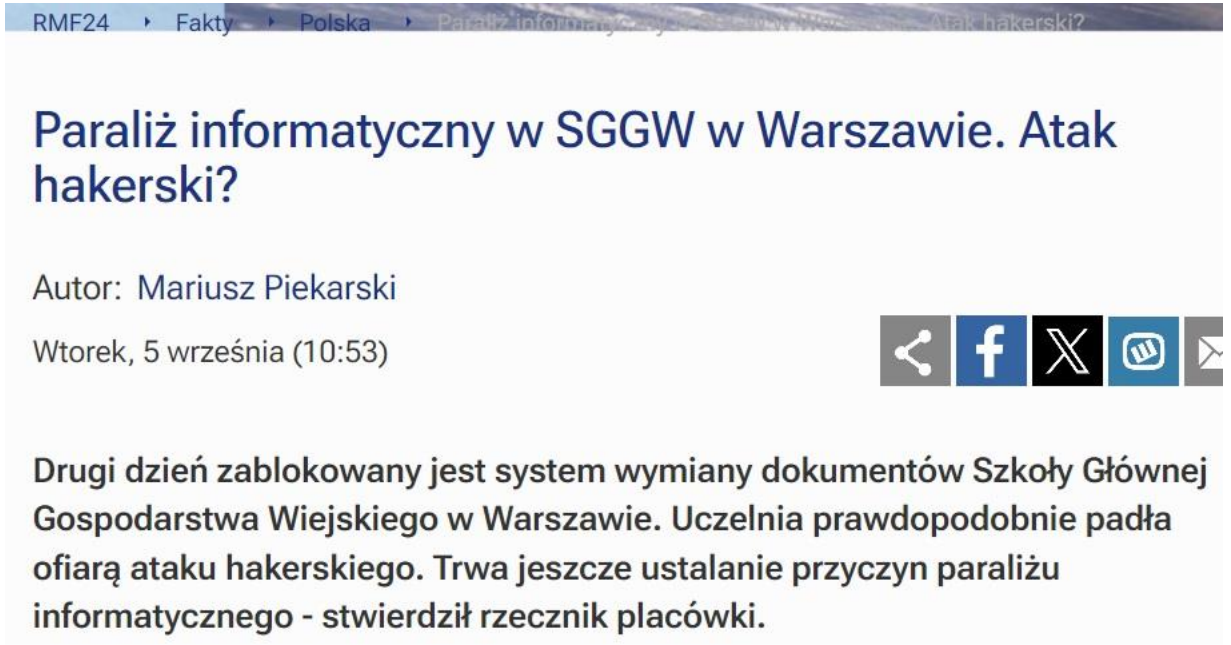
Mam pytanie dotyczące korespondencji przez system IRK - czy istnieje w nim jakaś wygodna forma (zakładam przy tym, że kopiuj - wklej do zewnętrznego emaila taką nie jest) przesyłania dalej korespondencji do innych użytkowników IRK - przykładowo Państwa lub kolegów z wydziałowych komisji?

Pozdrawiam,
Krzysztof Świtała
WPiA UKSW

W przypadku pytań zadawanych przez kandydatów – nie ma możliwości dopisywania kogoś do rozmowy (a szkoda), taka możliwość jest tylko, gdy my piszemy do kandydata.
Niestety pozostaje nam przesyłanie linków.



SGGW – blokada systemu obiegu dokumentów poprzez ransomware szyfrujący pliki (9.2023)



RMF24 › Fakty › Polska › Paraliż informatyczny ... Atak hakerski?

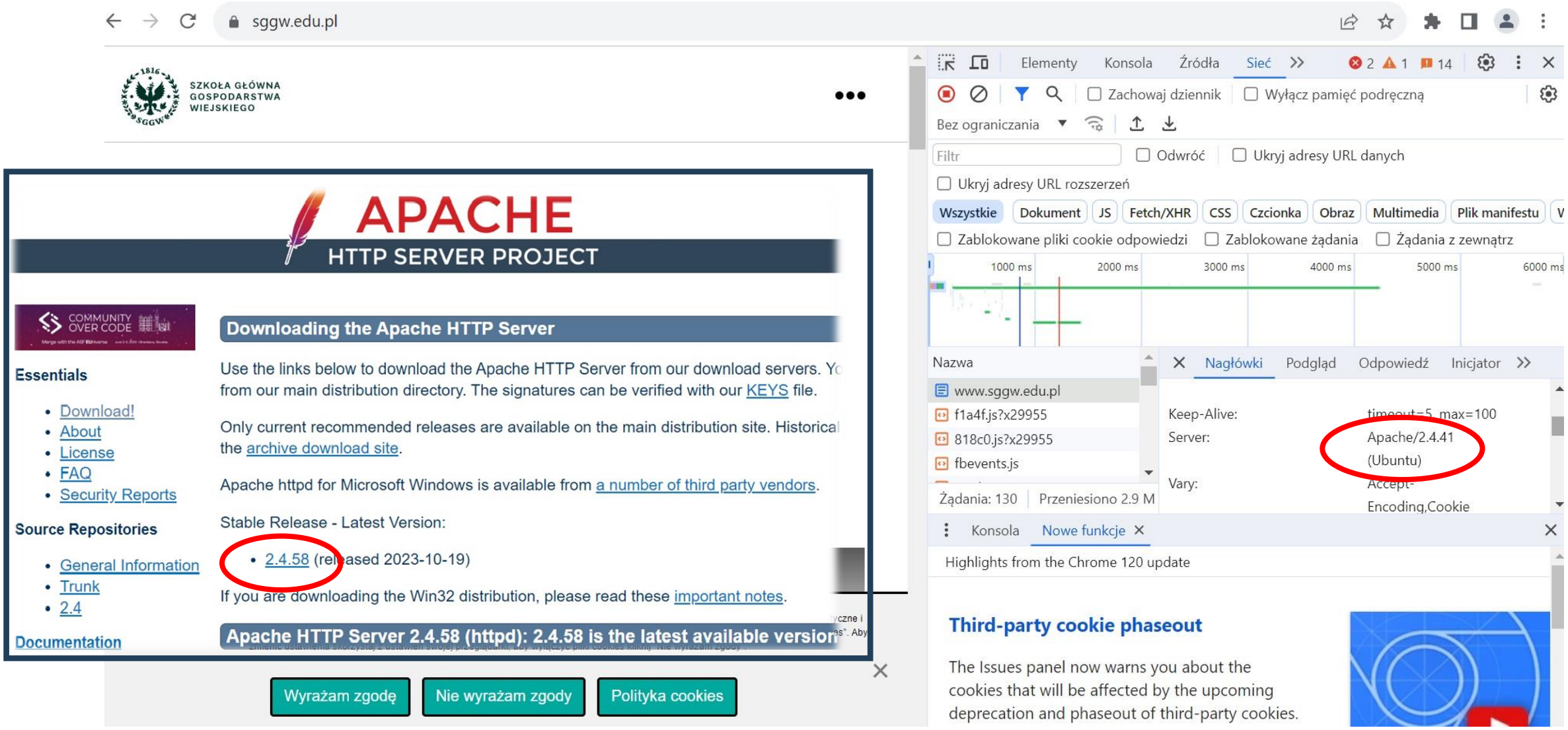
Paraliż informatyczny w SGGW w Warszawie. Atak hakerski?

Autor: Mariusz Piekarski

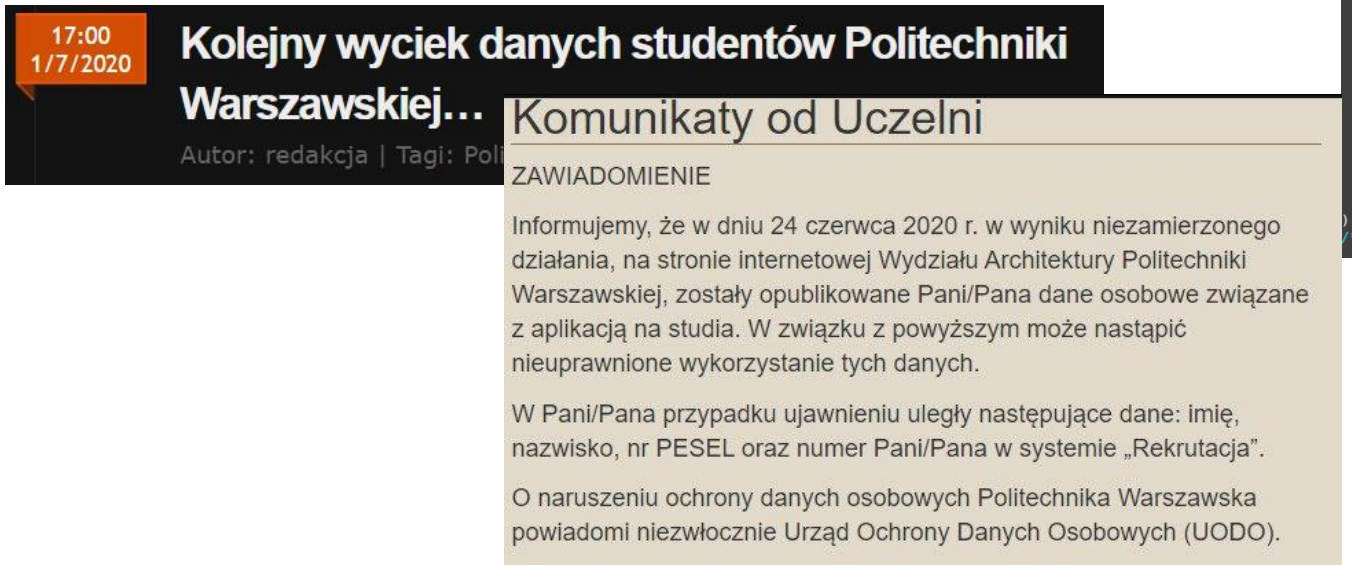
Wtorek, 5 września (10:53)

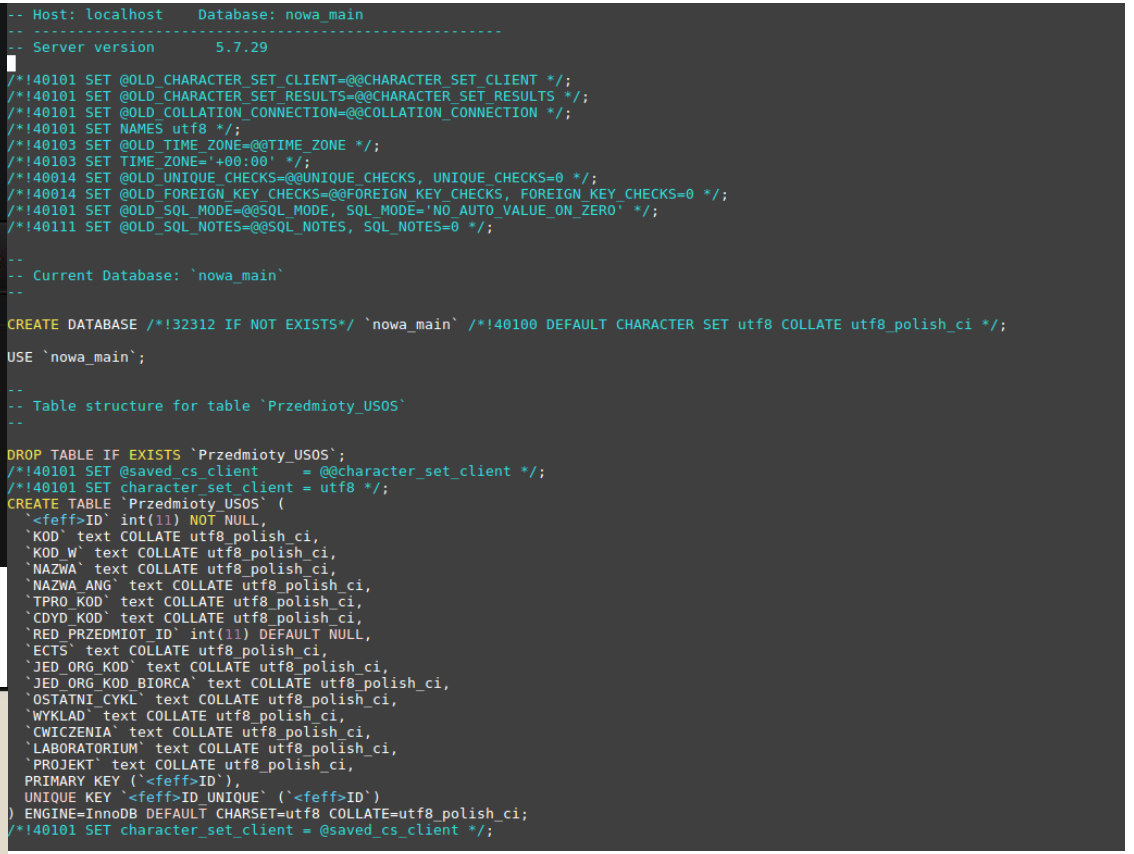
Drugi dzień zablokowany jest system wymiany dokumentów Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie. Uczelnia prawdopodobnie padła ofiarą ataku hakerskiego. Trwa jeszcze ustalanie przyczyn paraliżu informatycznego - stwierdził rzecznik placówki.

Strona WWW SGGW – ujawnienie konfiguracji serwera WWW w nagłówkach HTTP



Politechnika Warszawska – wycieki danych w 2020 r.





```
-- Host: localhost    Database: nowa_main
-- ------------------------------------------------------
-- Server version       5.7.29

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Current Database: `nowa_main`
--

CREATE DATABASE /*!32312 IF NOT EXISTS*/ `nowa_main` /*!40100 DEFAULT CHARACTER SET utf8 COLLATE utf8_polish_ci */;

USE `nowa_main`;

--
-- Table structure for table `Przedmioty_USOS`
--

DROP TABLE IF EXISTS `Przedmioty_USOS`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `Przedmioty_USOS` (
  `<feff>ID` int(11) NOT NULL,
  `KOD` text COLLATE utf8_polish_ci,
  `KOD_W` text COLLATE utf8_polish_ci,
  `NAZWA` text COLLATE utf8_polish_ci,
  `NAZWA_ANG` text COLLATE utf8_polish_ci,
  `TPRO_KOD` text COLLATE utf8_polish_ci,
  `CDYD_KOD` text COLLATE utf8_polish_ci,
  `RED_PRZEDMIOT_ID` int(11) DEFAULT NULL,
  `ECTS` text COLLATE utf8_polish_ci,
  `JED_ORG_KOD` text COLLATE utf8_polish_ci,
  `JED_ORG_KOD_BIORCA` text COLLATE utf8_polish_ci,
  `OSTATNI_CYKL` text COLLATE utf8_polish_ci,
  `WYKLAD` text COLLATE utf8_polish_ci,
  `CWICZENIA` text COLLATE utf8_polish_ci,
  `LABORATORIUM` text COLLATE utf8_polish_ci,
  `PROJEKT` text COLLATE utf8_polish_ci,
  PRIMARY KEY (`<feff>ID`),
  UNIQUE KEY `<feff>ID_UNIQUE` (`<feff>ID`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_polish_ci;
/*!40101 SET character_set_client = @saved_cs_client */;
```

Dziękujemy za uwagę