Zeszyty Naukowe
Zbliżenia Cywilizacyjne
XVII (3)/2021

DOI: https://doi.org/10.21784/ZC.2021.014

BARTOSZ SEKULSKI[1], DANIEL KORDYLEWSKI[1],
KRYSTIAN ORENKIEWICZ[1], MATEUSZ KALUZIŃSKI[1],
DOMINIKA LISIAK-FELICKA[2]
[1] Studenckie Koło Naukowe NET przy PUZ we Włocławku
[2] Uniwersytet Łódzki

Wybrane aspekty cyberbezpieczeństwa. Bezpieczeństwo fizyczne pracowni komputerowych

Selected aspects of cybersecurity. Physical security of computer labs

Streszczenie
Artykuł poświęcony został zagadnieniom związanym z cyberbezpieczeństwem. Zawiera prezentację przykładów ataków cyberprzestępców na instytucje edukacyjne. Ponadto autorzy skupili się na kwestiach bezpieczeństwa fizycznego, które dość często jest bagatelizowanym elementem systemu zarządzania bezpieczeństwem informacji.
W artykule przedstawione zostały działania zrealizowane przez członków Studenckiego Koła Naukowego NET związanych z projektowaniem i organizowaniem zaplecza sprzętowego i sieciowego pracowni komputerowych w nowym kampusie Państwowej Uczelni Zawodowej we Włocławku – Centrum Nauk Technicznych i Nowoczesnych Technologii.
Słowa kluczowe: cyberbezpieczeństwo, bezpieczeństwo fizyczne, sektor edukacyjny

Abstract
This article is devoted to issues related to cybersecurity. It contains a presentation of examples of attacks by cybercriminals on educational institutions. Also, the authors focused on physical security issues, which is quite often an underestimated element of an information security management system.
The article presents the activities conducted by the members of the NET Students' Scientific Organisation related to the design and organisation of equipment and network facilities of computer laboratories in the new campus of the State Vocational University in Włocławek – Centre for Technical Sciences and Modern Technologies.
Keywords: cybersecurity, physical security, education sector

1. Wprowadzenie

Cyberbezpieczeństwo zgodnie z definicją zawartą w normie ISO/IEC 270032-3.20 to zachowanie poufności, integralności i dostępności informacji w cyberprzestrzeni. Definicja ta jest zaadoptowaną wersją definicji bezpieczeństwa informacji w obszarze cyberprzestrzeni[1].

Na podstawie raportów przygotowanych przez zespół CERT.PL można zauważyć gwałtowny wzrost incydentów w cyberprzestrzeni. Liczby incydentów zarejestrowanych przez ten zespół zostały przedstawione na wykresie 1. Ponadto dominującym typem ataku zarówno w roku 2018 i 2019 były oszustwa komputerowe. Na kolejnych miejscach znalazło się oprogramowanie złośliwe oraz obraźliwe i nielegalne treści (zobacz wykres 2)[2].

Incydenty nie omijają również sektora edukacyjnego. Według raportu firmy Check Point dynamicznie wzrasta liczba ataków na instytucje edukacyjne i badawcze w USA, Europie oraz Azji[3]. W Polsce „w pierwszym tygodniu września identyfikowano średnio 837 prób ataków na pojedynczą jednostkę edukacyjną, o trzydzieści więcej niż miesiąc wcześniej. W ostatnim kwartale szczyt ataków zaobserwowano w trzecim tygodniu lipca, kiedy to przeprowadzono średnio 955 ataków". Szkoły i uczelnie są atakowane przez *malware* typu *botnet*, *cryptominery*, trojany bankowe i *infostealery*.

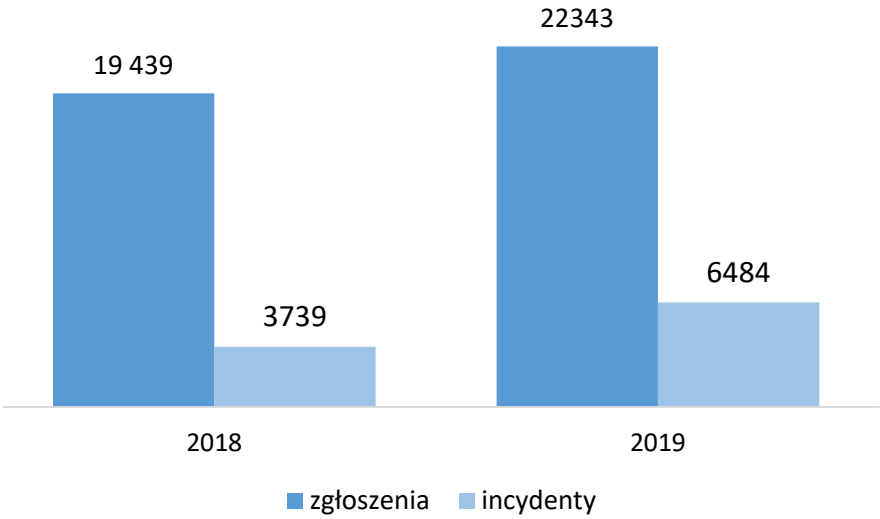
---

1 ISO-IEC 27032 ISO/IEC 27032:2012 *Information technology – Security techniques – Guidelines for cybersecurity*, Lisiak-Felicka D., Szmit M., *Cyberbezpieczeństwo administracji publicznej w Polsce*, European Association of Security, Kraków 2006, s. 48-53, R. von Solms, J. van Niekerk, *From information security to cyber security*. Computers & Security, Volume 38, October 2013, Pages 97-102, https://doi.org/10.1016/j.cose.2013.04.004.

2 CERT.PL, *Krajobraz bezpieczeństwa polskiego Internetu*, Raport roczny 2019 z działalności CERT Polska, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf [dostęp: 20.11.2020].

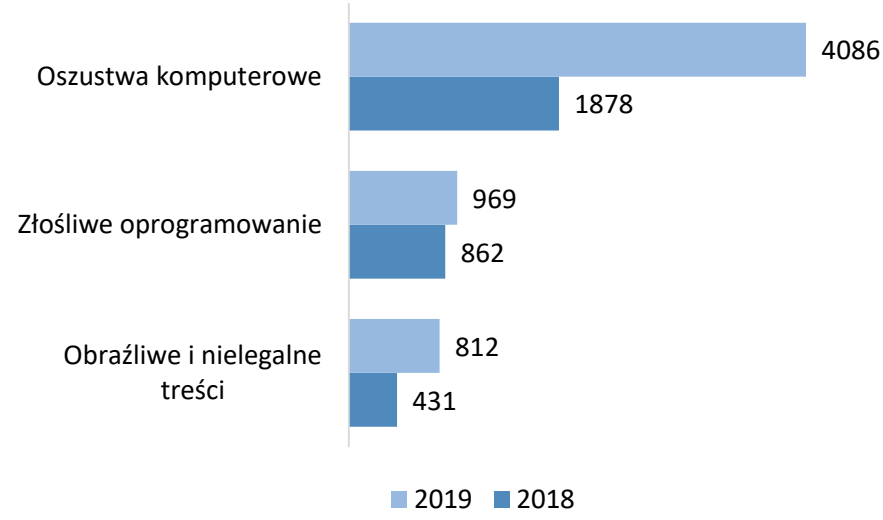
3 Check Point Blog, *Not for higher education: cybercriminals target academic & research institutions across the world*, https://blog.checkpoint.com/2020/09/15/not-for-higher-education-cybercriminals-target-academic-research-institutions-across-the-world/ [dostęp: 20.11.2020], A. Ścibor, *Polskie szkoły i uczelnie atakowane nawet 950 razy w tygodniu*, https://avlab.pl/polskie-szkoly-i-uczelnie-atakowane-nawet-950-razy-w-tygodniu/ [dostęp: 20.11.2020], B. Igielska, *Coraz więcej hakerskich ataków na szkoły i uczelnie*, https://www.prawo.pl/oswiata/hakerskie-ataki-na-szkoly-i-uczelnie-w-czasie-pandemii-jest-ich,503340.html [dostęp: 20.11.2020].

Wykres 1. Liczby zgłoszeń i incydentów zarejestrowanych przez CERT.PL w latach 2018-2020



Źródło: opracowanie własne na podstawie raportów CERT.PL

Wykres 2. Dominujące typy incydentów w latach 2018-2019



Źródło: opracowanie własne na podstawie raportów CERT.PL

W ostatnim czasie pojawia się coraz więcej ataków cyberprzestępców w sektorze edukacyjnym. Jak podaje PAP w lipcu 2020 co najmniej 10 uniwersytetów w Wielkiej Brytanii, USA i Kanadzie zostało zaatakowanych oprogramowaniem *ransomwere*. Skutkiem ataku była kradzież danych osobowych studentów oraz absolwentów[4].

Również w Polsce w roku 2020 miało miejsce kilka spektakularnych ataków cyberprzestępców na uczelnie.

W lutym 2020 roku została zaatakowana strona internetowa Uniwersytetu Rzeszowskiego. Pojawiła się na niej fałszywa informacja o zamknięciu uczelni w związku z zagrożeniem koronawirusem[5].

W kwietniu 2020 roku przeprowadzono atak na stronę internetową Akademii Sztuki Wojennej. Umieszczono na niej został umieszczony spreparowany list rektora, skierowany do wojskowych. List ten zawierał wiele szkodliwych informacji nie tylko dla dobrego imienia rektora-komendanta i uczelni, ale również dla wizerunku całego kraju[6].

W tym samym miesiącu zaatakowano poznańskie Collegium Da Vinci (CDV) oraz warszawski Uniwersytet SWPS. Strona uczelni CDV nie była aktywna, a pracownicy otrzymali informację o zresetowaniu haseł. Uczelnia wyjaśniła, że nastąpił nieautoryzowany dostęp do zasobów, a celem włamania było zaszyfrowanie danych i żądanie okupu w zamian za ich odblokowanie. Równocześnie podobny atak miał miejsce na Uniwersytecie SWPS, w związku z tym że uczelnia ta razem z CDV wykorzystują tą samą infrastrukturę sieciową[7].

---

4 *Oxford i co najmniej 9 innych uczelni ofiarami ataku hakerskiego*, https://www.pap.pl/pap-technologie/688389%2Coxford-i-co-najmniej-9-innych-uczelni-ofiarami-ataku-hakerskiego.html [dostęp: 20.11.2020].

5 Atak hakerski na stronę internetową Uniwersytetu Rzeszowskiego, https://rzeszow24.pl/koronawirus-atak-hakerski-na-strone-internetowa-uniwersytetu-rzeszowskiego-foto-9179-00r2kc/ [dostęp: 20.11.2020].

6 Akademia Sztuki Wojennej obiektem działań dezinformacyjnych. Próba osłabienia relacji z USA, https://www.cyberdefence24.pl/akademia-sztuki-wojennej-obiektem-dzialan-dezinformacyjnych-proba-oslabienia-relacji-z-usa [dostęp: 20.11.2020].

7 A. Haertle, *Poważny incydent bezpieczeństwa na uczelniach Collegium Da Vinci i SWPS*, https://zaufanatrzeciastrona.pl/post/powazny-incydent-bezpieczenstwa-na-uczelniach-collegium-da-vinci-i-swps/ [dostęp: 20.11.2020].

W maju miał miejsce wyciek danych osobowych studentów i pracowników Politechniki Warszawskiej[8].

Dane ponad 5 tys. osób zostały wykradzione z platformy administracyjnej Ośrodka Kształcenia na Odległość (OKNO). W przypadku studentów mogło dojść do ujawnienia danych m.in.: imienia i nazwiska, serii i nr dowodu osobistego, nr PESEL, adresu, imiona rodziców, nazwisko rodowe matki, datę i miejsce urodzenia, adresu e-mail, nazwy użytkownika, telefonu oraz numeru NIP w przypadku studentów, którym wystawione zostały faktury. W przypadku nauczycieli akademickich: imię, nazwisko oraz adres e-mail. Uczelnia zgłosiła ten fakt Urzędowi Ochrony danych Osobowych oraz policji[9].

Co więcej, w lipcu 2020 roku, miał miejsce ponowny atak na Politechnikę Warszawską. Tym razem zaatakowano Wydział Architektury i wykradzione zostały dane z systemu Rekrutacja[10].

Powyższe wskazuje, że niezwykle istotne jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji w instytucjach edukacyjnych i badawczych. W niniejszym artykule przedstawiono jeden z aspektów zabezpieczeń przed incydentami związanymi z bezpieczeństwem informacji – bezpieczeństwo fizyczne[11].

---

8 A. Haertle, *Poważny wyciek wielu danych osobowych studentów Politechniki Warszawskiej*, https://zaufanatrzeciastrona.pl/post/powazny-wyciek-wielu-danych-osobowych--studentow-politechniki-warszawskiej/ [dostęp: 20.11.2020]. M. Maj, *Wyciek danych z Politechniki Warszawskiej – nazwiska, dane kontaktowe, oceny*, https://niebezpiecznik.pl/post/wyciek-danych-z-politechniki-warszawskiej-nazwiska-dane-kontaktowe-oceny/ [dostęp: 20.11.2020].

9 *Duży wyciek danych na Politechnice Warszawskiej*, https://www.bankier.pl/wiadomosc/Duzy-wyciek-danych-na-Politechnice-Warszawskiej-7878720.html [dostęp: 20.11.2020].

10 *Kolejny wyciek danych studentów Politechniki Warszawskiej…,* https://niebezpiecznik.pl/post/kolejny-wyciek-danych-studentow-politechniki-warszawskiej/ [dostęp: 20.11.2020].

11 E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, B. Klepacki, *Information security assessment in public administration*, Computers & Security, Volume 90, March 2020, 101709, https://doi.org/10.1016/j.cose.2019.101709, A. V. Singar, K. B., Akhilesh K.B. *Role of Cyber-security in Higher Education*. In: Akhilesh K., Möller D. (eds) Smart Technologies. Springer, Singapore. https://doi.org/10.1007/978-981-13-7139-4_19.

2. Bezpieczeństwo fizyczne

Ten element ma duże znaczenie, często jednak jest pomijany lub marginalizowany przy planowaniu systemu zarządzania bezpieczeństwem informacji. Zgodnie z normą ISO/IEC 27002[12] bezpieczeństwo fizyczne i środowiskowe podzielone zostało na dwa elementy: obszary bezpieczne i sprzęt. Celem zabezpieczenia odnoszącego się do obszarów bezpiecznych jest zapobieganie nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w informacjach i środkach przetwarzania informacji należących do organizacji.

Szczegółowe zalecenia odnoszą się do fizycznej granicy obszaru bezpiecznego, zabezpieczania wejść, biur, pomieszczeń i obiektów, ochrony przed zagrożeniami zewnętrznymi i środowiskowymi, pracy w obszarach bezpiecznych, obszarach dostaw i załadunku.

Celem zabezpieczenia odnoszącego się do sprzętu jest zapobieganie utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji.

Szczegółowe zalecenia odnoszą się do lokalizacji i ochrony sprzętu, systemów wspomagających, bezpieczeństwa okablowania, konserwacji sprzętu, wynoszenia aktywów, bezpieczeństwa sprzętu i aktywów poza siedzibą, bezpiecznego zbywanie lub przekazywania do ponownego użycia, pozostawiania sprzętu użytkownika bez opieki, polityki czystego biurka i czystego ekranu.

3. Cel, metoda i zakres prac

Celem artykułu jest analiza wybranych aspektów cyberbezpieczeństwa w funkcjonowaniu wszystkich podmiotów związanych z działalnością edukacyjną. Do realizacji postawionego celu wykorzystana została metoda badania dokumentów, w tym raportów zespołu reagowania na incydenty komputerowe CERT.PL oraz artykułów dotyczących incydentów związanych z bezpieczeństwem informacji, jakie miały miejsce na uczelniach wyższych.

[12] PN-EN ISO/IEC 27002:2017-06, *Technika informatyczna -– Techniki bezpieczeństwa -– Praktyczne zasady zabezpieczania informacji.*

Ponadto zaprezentowano działania Studenckiego Koła Naukowego NET, którego członkowie w okresie przerwy letniej roku akademickiego 2019/2020 działali aktywnie wykonując prace przygotowawcze w nowoczesnych pracowniach komputerowych Centrum Nauk Technicznych i Nowoczesnych Technologii PUZ przy ulicy Energetyków 30 we Włocławku. Do wykonywanych prac należało między innymi:

- przygotowanie miejsca do pracy,
- zaplanowanie oraz rozmieszczenie stanowisk komputerowych zgodnie z zasadami ergonomii,
- montaż i konfiguracja sprzętu,
- rozplanowanie, przygotowanie i rozmieszczenie okablowania,
- konfiguracja urządzeń sieciowych,
- instalacja systemów, sterowników i oprogramowania,
- utworzenie kopii zapasowych,
- sporządzenie stosownej dokumentacji,
- sporządzanie specyfikacji do przetargu,
- testy.

Przed przystąpieniem do prac członkowie koła odbyli szkolenia z zakresu BHP oraz ochrony danych osobowych.

4. Wykonane prace w pracowni sieciowej

Priorytetem podczas prac była pracownia technologii sieciowych. Podobnie jak w pozostałych pracowniach, liczba przyłączy energetycznych oraz gniazdek sieciowych i ich rozmieszczenie stanowiło trudność w rozplanowaniu stanowisk. Zadanie tego typu wymaga skupienia i nie działania w pośpiechu. Przy kilkunastu komputerach łatwo o sytuację, w której podłączy się wszystko „na styk" uwzględniając przy tym nawet gniazdko potrzebne do szafy, a finalnie okazuje się że trzeba całkiem zmienić koncepcję z powodu przeoczonego rzutnika. Należy pamiętać, że nie można podłączać zbyt wielu urządzeń pod jedno przyłącze. Mogłoby to skutkować nawet uszkodzeniem instalacji elektrycznej.

W kolejnych sekcjach przedstawiono m.in.: charakterystykę stacji roboczych w pracowni sieciowej, wykaz zainstalowanego oprogramo-

wania, sposób uwierzytelniania użytkowników, budowę wybranych elementów infrastruktury sieciowej, tworzenie kopii zapasowych.

4.1. Sprzęt, oprogramowanie i uwierzytelnianie użytkowników

Pracownia sieciowa wyposażona jest w nowoczesne i zaawansowane urządzenia oraz narzędzia sieciowe i 15 stanowisk komputerowych z systemami:

- Windows 10,
- Windows Server 2019,
- Linux Debian.

Ten zestaw systemów niezbędny jest do nauki administrowania siecią. Przeciętny użytkownik korzysta z jednego (maksymalnie dwóch) systemów. Przy takiej liczbie systemów operacyjnych na jednej maszynie warto zapoznać się ze schematami partycjonowania. Wyróżniamy: MBR (ang. *Master Boot Record*) – w systemach opartych na BIOS i GPT (ang. *GUID Partition Table*) – w systemach opartych na UEFI (ang. *Unified Extensible Firmware Interface*). Są to dwa różne sposoby przechowywania informacji partycji dysku. Zasadniczą różnicą między nimi jest to, że MBR jest znacznie ograniczony w stosunku do GPT. MBR obsługuje maksymalnie 2TB pojemności dysku i pozwala na utworzenie maksymalnie 4 partycji podstawowych. Chcąc utworzyć kolejne partycje trzeba utworzyć partycję rozszerzoną, a w niej partycje logiczne. GPT takich ograniczeń nie posiada. Obsługuje znacznie większe dyski i pozwala na nieograniczoną ilość partycji podstawowych.

Dla powyższych systemów potrzebne były dwie partycje dla Windows 10 (C, D), jedna dla Windows Server 2019 (R), 3 dla systemu Debian 10 (główna, rozruchowa, *home*) oraz jedna dla obrazu dysku. Nie ulega więc wątpliwości, że MBR tego nie udźwignie. Niestety większość ze stanowisk z fabrycznie zainstalowanym Windows 10, miała właśnie ten schemat partycjonowania. Prawidłowa konwersja między jednym a drugim wiąże się z wymazaniem całej zawartości dysku twardego. Posłużył do tego prosty (i skuteczny) program Diskpart. Ponowna instalacja domyślnego systemu i kompletu sterowników na wielu urzą-

dzeniach była bardzo czasochłonna. Mając już możliwość utworzenia niezbędnych partycji warto zastanowić się nad kolejnością instalowanych systemów. Zadecydowano o zainstalowaniu Debiana na samym końcu. Program rozruchowy GRUB po zaktualizowaniu bez przeszkód odnajduje Windows *bootloader*, co jest istotne dla łatwego przełączania między systemami w menu rozruchowym.

Zdarza się, że po aktualizacji jednego z microsoftowych systemów *bootloader* próbuje nadpisać GRUBa i przy starcie komputera zamiast klasycznego menu wyboru wyświetla się tzw. *Metrobootloader*. Wówczas wystarczy z poziomu Windows 10 / Windows Server uruchomić konsolę jako administrator i wpisać:

bcdedit /set {default} bootmenupolicy legacy

Komputery w pracowni sieciowej będą się łączyć przez sieć Wi-Fi. Ze względów bezpieczeństwa serwerów nie przyłącza się do sieci bezprzewodowo. Dlatego też w systemach Windows Server domyślnie moduł bezprzewodowy nie działa. Ponadto wiele bezprzewodowych kart sieciowych nie ma sterowników dla tego systemu. Rozwiązaniem tego problemu było zainstalowanie funkcji serwera związanej z obsługą sieci bezprzewodowej oraz ręczne wgranie sterowników (zdarza się że sterownik może poprawnie działać na niekompatybilnym systemie, ale system nie chce go przyjąć zwracając komunikat o niekompatybilności). W takiej sytuacji stosuje się sztuczkę polegającą na „oszukaniu" komputera. Wystarczy wybrać odpowiednią kartę sieciową w menu producentów przy ręcznej instalacji, a następnie wskazać dokładną lokalizację sterownika.

Na koniec zainstalowano programy:

- Wireshark – (do analizy ruchu w sieci),
- Cisco Packet Tracer – (do nauki projektowania sieci),
- Pakiet Office 2019.

Sprzęt komputerowy w pracowni służy do nauki, podczas której studenci popełniają błędy. Niektóre z tych błędów wymagają ingerencji w systemy. Czas potrzebny do przywrócenia trzech systemów, ich sterowników, ról, funkcji i programów jest jedynie czasem straconym

dla studenta. Dlatego utworzona została na każdym stanowisku specjalna partycja na obraz całego dysku. Posłużył do tego program Acronis True Image 2017. Za pomocą tego narzędzia, uruchomionego z płyty utworzono obraz całego dysku twardego w jednym pliku. Na jednym z komputerów przeprowadzono testy. Wszystkie trzy systemy zostały przywrócone do „stanu idealnego" w trakcie jednej operacji w około 8 minut. Jedyną dodatkową czynnością, którą należało wykonać ponowne nadpisanie *bootloader* przez GRUB, aby system Linux był widoczny w menu rozruchowym. Instrukcja do przywrócenia obrazu dysku i nadpisania programu rozruchowego została dołączona do dokumentacji.

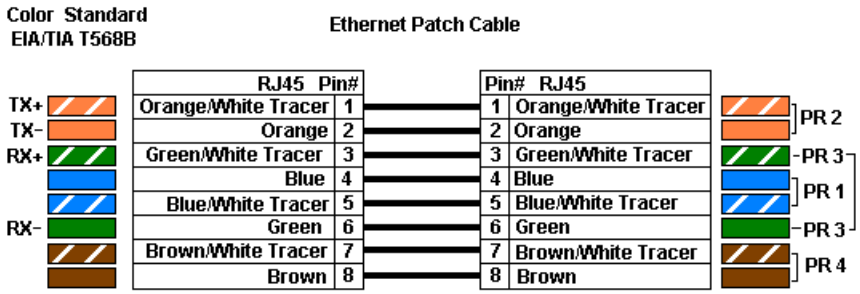
Na serwerze zainstalowano usługę domenową Active Directory, która umożliwia centralnie (z serwera pełniącego funkcję kontrolera domeny) zarządzać kontami użytkowników w sieci, nadawać im uprawnienia do zasobów sieciowych oraz konfigurować stacje robocze. Kontroler domeny ułatwia również administratorowi zarządzanie zabezpieczeniami. W celu ochrony zasobów sieciowych utworzone zostały zabezpieczenia w ramach zasad grupowych (GPO). W ten sposób można kontrolować: uwierzytelnianie użytkowników, zasoby, z których użytkownik chce skorzystać, aktywność użytkowników, członkostwo w grupach. Logowanie użytkowników w pracowni sieciowej odbywa się z wykorzystaniem kont domenowych.

4.2. Elementy infrastruktury sieciowej

Kolejne zadanie polegało na podłączeniu do Internetu wszystkich stacji roboczych znajdujących się w salach komputerowych. Było to możliwe jedynie za pomocą kabla sieciowego LAN *Ethernet*. Skrętka jest rodzajem kabla sygnałowego służącego do przesyłania informacji, który zbudowany jest z jednej lub więcej par skręconych ze sobą żył w celu eliminacji wpływu zakłóceń elektromagnetycznych oraz zakłóceń wzajemnych, zwanych przesłuchami. Skręcenie żył powoduje równocześnie zawężenie pasma transmisyjnego. W celu połączenia stacji roboczych z Internetem zarabiano skrętkę typu T568B ekranowaną z folią (F/UTP) wykorzystując przewód kategorii 5e przeznaczony do

wykonywania instalacji wewnątrz budynków. Ekran wykonany z folii aluminiowej w większym stopniu pozwala zniwelować przesłuchy i zakłócenia pochodzące ze środowiska zewnętrznego. Do zarabiania kabli użyto zaciskarki, wtyczek RJ45 dla kategorii 5e oraz testera okablowania sieci LAN. Odpowiednie ułożenie żył pokazuje rysunek 3.

Rysunek 3. Układ żył standardu T568B



Źródło: http://www.egs.com.pl/drupal/RJ45

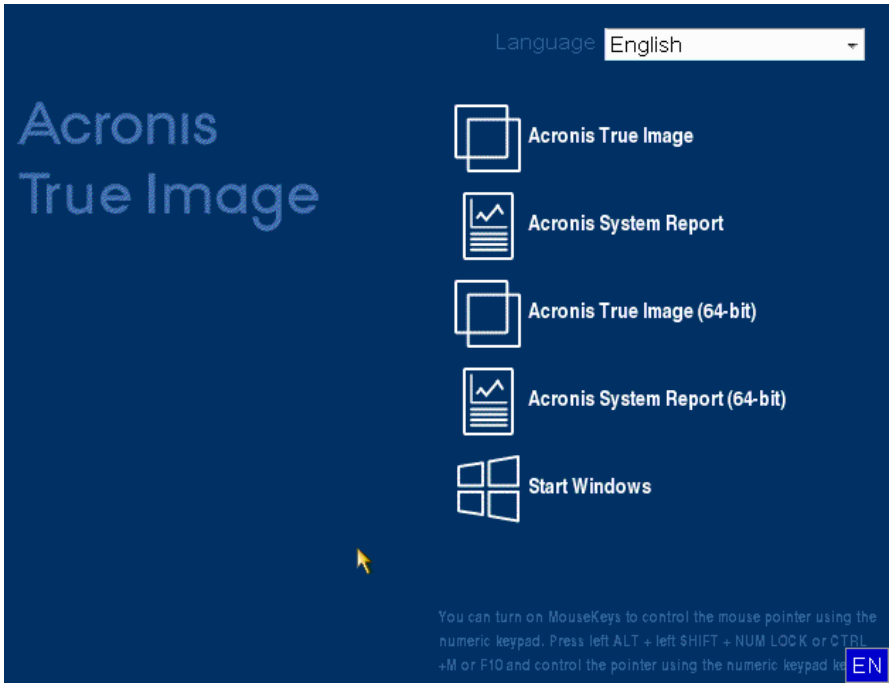
Po ułożeniu żył w odpowiedni sposób należy je wyrównać, a następnie w odpowiedni sposób włożyć do wtyczki i zacisnąć. Podczas zarabiania kabla służącego do komunikacji pomiędzy projektorem a komputerem wykładowcy, wykorzystano okablowanie kategorii 6. Układ żył się nie zmienił jednak dla tego typu kabla należało użyć specjalnych wtyczek przeznaczonych do tej kategorii. Przy próbie użycia innych końcówek wykonanie zadania było bardzo problematyczne.

4.3. Kopie zapasowe

Tworzenie kopii zapasowych określa zasady wykonywania, przechowywania i testowania kopii zapasowych oraz odzyskiwania z nich danych i systemów informatycznych, w celu zapewnienia integralności i dostępności informacji oraz środków przetwarzania informacji. W tym celu wykorzystano program Acronis True Image 2017, który umożliwia tworzenie obrazów dysków twardych, wybranych partycji lub plików i folderów. Program oferuje dwa rodzaje kreowania obrazów. Standardowy umożliwia tworzenie obrazów całych dysków twardych, wraz

z systemami operacyjnymi, aplikacjami, ustawieniami użytkownika i wszystkimi danymi. W przypadku utraty całości lub części danych możliwe jest przywracanie stanu komputera bez konieczności ponownej instalacji systemu operacyjnego. Ponadto program pozwala na tworzenie i przywracanie obrazów indywidualnych plików i folderów, takich jak folder Moje Dokumenty lub określony plik. Acronis umożliwia tworzenie kopii zapasowych na dwa sposoby z poziomu Windows lub DOS. W opisywanym przypadku tworzono obrazy z poziomu systemu DOS. Aby to wykonać należy włożyć płytę lub pendrive z programem Acronis a następnie wybrać bootowanie z danego nośnika przy uruchamianiu komputera. Kiedy uruchomi się program należy wybrać Acronis True Image, aby wejść do programu (rysunek 3).

Rysunek 4. Panel startowy programu Acronis True Image 2017



W programie wyświetlają się okienka podobne jak w systemie Windows. Aby zrobić kopię zapasową systemu należy wybrać opcję *Backup*, a następnie dyski i partycja.

Kolejnym krokiem jest wybór dysku, na którym znajduje się system, a następnie zaznaczenie opcji tworzenia nowej kopii lub dodania plików do wcześniej wykonanego obrazu. Dalej należy wybrać miejsce, w którym obraz ma zostać zapisany. Może to być dysk komputera lub zewnętrzny nośnik. Po wyborze miejsca należy nadać nazwę kopii lub wygenerować domyślną nazwę. Po zatwierdzeniu nazwy kopii pojawi się okienko z informacją na temat obrazu. Następnie należy kliknąć „*Proceed*", aby program zaczął tworzenie kopii zapasowej dysku.

Za pomocą programu Acronis można również przywrócić obrazy systemu w przypadku gdy dane zostaną utracone. Aby to zrobić należy uruchomić program tak samo jak w przypadku tworzenia kopii, a następnie wybrać *Recovery*. Następnie należy wybrać utworzoną wcześniej kopię zapasową z dysku lub nośnika zewnętrznego i zaznaczyć opcję *Recover*. Konieczne jest zaznaczenie opcji przywrócenia całego dysku oraz partycji. W ostatnim kroku program wyświetli okienko z informacjami. Należy kliknąć „*Proceed*" aby program rozpoczął przywracanie.

Program Acronis True Image pozwala na tworzenie i przywracanie kopii zapasowych zarówno całych dysków jak i pojedynczych folderów w łatwy i intuicyjny sposób. Dużą zaletą programu jest również to, że może on działać niezależnie od systemu.

5. Podsumowanie i wnioski

Na podstawie przedstawionych wyników raportów oraz danych o incydentach można zauważyć znaczący wzrost liczby ataków cyberprzestępców w sektorze edukacyjnym. Istnieje zatem konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa informacji i zapewnienia ciągłości działania. Są to ważne aspekty w funkcjonowaniu wszystkich podmiotów związanych z działalnością edukacyjną.

W ramach prac Studenckiego Koła Naukowego NET przeprowadzono działania związane z projektowaniem i organizowaniem zaplecza

sprzętowego i sieciowego pracowni komputerowych w nowym budynku Państwowej Uczelni Zawodowej. Wykonywane prace umożliwiły zdobycie umiejętności praktycznych. Niektóre czynności stwarzały pewne trudności. W artykule przedstawiono rozwiązania i zamieszczono wskazówki, które mogą być przydatne dla administratorów sieci komputerowych bądź osób wykonujących podobne zadania. Wykonane prace, począwszy od ustawienia sprzętu, zaprojektowania i wykonania okablowania, instalacji i konfiguracji stanowisk komputerowych po tworzenie kopii zapasowych, mają bezpośredni związek z zapewnieniem cyberbezpieczeństwa pracowni komputerowych w aspekcie fizycznym i środowiskowym.

W ramach dalszych zadań Studenckiego Koła Naukowego NET planowane są kolejne prace związane z konfiguracją urządzeń sieciowych, konfiguracją sieci Wi-Fi na holu budynku oraz prace w pozostałych pracowniach komputerowych.

Bibliografia

Bankier.pl, Duży wyciek danych na Politechnice Warszawskiej, https://www.bankier.pl/wiadomosc/Duzy-wyciek-danych-na-Politechnice-Warszawskiej-7878720.html

CERT.PL, Krajobraz bezpieczeństwa polskiego Internetu, Raport roczny 2019 z działalności CERT Polska, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf

Check Point Blog, Not for higher education: cybercriminals target academic & research institutions across the world, https://blog.checkpoint.com/2020/09/15/not-for-higher-education-cybercriminals-target-academic-research-institutions-across-the-world/

Cyberdefence24.pl, Akademia Sztuki Wojennej obiektem działań dezinformacyjnych. Próba osłabienia relacji z USA, https://www.cyberdefence24.pl/akademia-sztuki-wojennej-obiektem-dzialan-dezinformacyjnych-proba-oslabienia-relacji-z-usa

Haertle A., Poważny incydent bezpieczeństwa na uczelniach Collegium Da Vinci i SWPS, https://zaufanatrzeciastrona.pl/post/powazny-incydent-bezpieczenstwa-na-uczelniach-collegium-da-vinci-i-swps/

Haertle A., Poważny wyciek wielu danych osobowych studentów Politechniki Warszawskiej, https://zaufanatrzeciastrona.pl/post/powazny-wyciek-wielu-danych-osobowych-studentow-politechniki-warszawskiej/

Igielska B., Coraz więcej hakerskich ataków na szkoły i uczelnie, https://www.prawo.pl/oswiata/hakerskie-ataki-na-szkoly-i-uczelnie-w-czasie-pandemii-jest-ich,503340.html

ISO-IEC 27032 ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity,

Lisiak-Felicka D., Szmit M., Cyberbezpieczeństwo administracji publicznej w Polsce, European Association of Security, Kraków 2006, s. 48-53,

Maj M., Wyciek danych z Politechniki Warszawskiej – nazwiska, dane kontaktowe, oceny, https://niebezpiecznik.pl/post/wyciek-danych-z-politechniki-warszawskiej-nazwiska-dane-kontaktowe-oceny/

Niebiezpiecznik.pl, Kolejny wyciek danych studentów Politechniki Warszawskiej…, https://niebezpiecznik.pl/post/kolejny-wyciek-danych-studentow-politechniki-warszawskiej/

PAP.PL, Oxford i co najmniej 9 innych uczelni ofiarami ataku hakerskiego, https://www.pap.pl/pap-technologie/688389%2Coxford-i-co-najmniej-9-innych-uczelni-ofiarami-ataku-hakerskiego.html

PN-EN ISO/IEC 27002:2017-06, Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji.

Rzeszów.pl, Atak hakerski na stronę internetową Uniwersytetu Rzeszowskiego, https://rzeszow24.pl/koronawirus-atak-hakerski-na-strone-internetowa-uniwersytetu-rzeszowskiego-foto-9179-00r2kc/

Ścibor A., Polskie szkoły i uczelnie atakowane nawet 950 razy w tygodniu, https://avlab.pl/polskie-szkoly-i-uczelnie-atakowane-nawet-950-razy-w-tygodniu/

Singar A.V., Akhilesh K.B., Role of Cyber-security in Higher Education. In: Akhilesh K., Möller D. (eds) Smart Technologies. Springer, Singapore 2020, https://doi.org/10.1007/978-981-13-7139-4_19

Szczepaniuk E. K., Szczepaniuk H., Rokicki T., Klepacki B., Information security assessment in public administration, Computers & Security, Volume 90, March 2020, 101709, https://doi.org/10.1016/j.cose.2019.101709,

Von Solms, R., Van Niekerk, J., From information security to cyber security. Computers & Security, Volume 38, October 2013, Pages 97-102. https://doi.org/10.1016/j.cose.2013.04.004