**Mariusz Śniadkowski, Agnieszka Jankowska**

# Zastosowanie programu Clonezilla dla bezpieczeństwa pracowni komputerowej = Clonezilla Software as a Method of Improving the Security in a Computer Laboratory

Edukacja - Technika - Informatyka nr 2(20), 330-334

2017

©Wydawnictwo UR 2017 „Edukacja – Technika – Informatyka" nr 2/20/2017
ISSN 2080-9069 www.eti.rzeszow.pl
ISSN 2450-9221 online DOI: 10.15584/eti.2017.2.43

**MARIUSZ ŚNIADKOWSKI**[1], **AGNIESZKA JANKOWSKA**[2]

# Zastosowanie programu Clonezilla dla bezpieczeństwa pracowni komputerowej

# Clonezilla Software as a Method of Improving the Security in a Computer Laboratory

[1] Doktor habilitowany, Politechnika Lubelska, Wydział podstaw Techniki, Katedra Metod i Technik Nauczania, Polska
[2] Magister inżynier, Politechnika Lubelska, Wydział podstaw Techniki, Polska

**Streszczenie**

Zapewnienie bezpieczeństwa systemu operacyjnego oraz niezawodności działania pracowni komputerowej jest zadaniem ciągle aktualnym. Nie można całkowicie wyeliminować możliwości uszkodzenia lub uzyskania nieuprawnionego dostępu do systemu operacyjnego. Można zastosować rozwiązania, które ograniczą lub będą przeciwdziałać niesprawności systemu komputerowego. Poniższy artykuł przedstawia charakterystykę zagrożeń systemu operacyjnego w szkolnej pracowni komputerowej oraz autorskiej aplikacji do tworzenia kopii bezpieczeństwa systemu operacyjnego przy wykorzystaniu darmowego programu Clonezilla.

**Słowa kluczowe:** pracownia komputerowa, bezpieczeństwo, Clonezilla

**Abstract**

Ensuring operating the system security and functional reliability of a computer laboratory is a virtually never-ending concern. It is impossible to completely eliminate the possibility of damage or unauthorised access to the operating system, but there are solutions designed to limit and prevent the risk of computer system malfunction. The present article discusses the particular threats to operating system integrity faced in an educational computer lab and describes the authors' operating system backup application developed with the use of free Clonezilla software.

**Keywords:** computer laboratory, security, Clonezilla software

## Wstęp

Bezpieczeństwo pracowni komputerowych, a zwłaszcza działania sytemu operacyjnego, jest zagadnieniem nadal aktualnym. Otwarte pozostaje pytanie o stopień zabezpieczenia pracowni komputerowej przed problemami systemu operacyjnego, które mogą utrudniać lub uniemożliwić realizację procesu dy-

daktycznego. Analizując dotychczasowe praktyki w dziedzinie zabezpieczania systemów komputerowych, należy stwierdzić, że nie można całkowicie wyeliminować możliwości uszkodzenia lub uzyskania nieuprawnionego dostępu do systemu operacyjnego. Dlatego należy przyjąć założenie, że jeśli nie można całkowicie i skutecznie zabezpieczyć systemów komputerowych przed uszkodzeniem lub zniszczeniem, powinno się zastosować takie rozwiązania, które ograniczą lub będą przeciwdziałać niesprawności systemu komputerowego.

**Analiza zagrożeń**

W literaturze przedmiotu zagrożenia bezpieczeństwa systemu w pracowni komputerowej mogą mieć charakter pasywny bądź aktywny. Można je dzielić na: fizyczne, komunikacyjne (sieciowe), związane z oprogramowaniem oraz związane z inżynierią społeczną.

Zagrożenia fizyczne. Jednym z zagrożeń mogących wystąpić w pracowni komputerowej są zagrożenia fizyczne, które mogą być pasywne lub aktywne. Do pasywnych należy zaliczyć wyładowania atmosferyczne, zalanie pracowni, pożar bądź awarię sprzętu komputerowego. Zagrożeniem aktywnym jest osoba nieupoważniona, która ma fizyczny dostęp do sprzętu komputerowego.

Zagrożenia tego typu można wyeliminować poprzez właściwe zaplanowanie instalacji elektrycznej, przeciwpożarowej i wodno-kanalizacyjnej. Przy braku zasilania stosuje się zasilacze awaryjne (UPS). Wszystkie te awarie są przypadkowe i nieprzewidywalne. Skutki ich można zminimalizować poprzez posiadanie kopii bezpieczeństwa danych czy posiadanie maszyn zapasowych. Natomiast urządzenia komputerowe powinny być zabezpieczane w zamkniętych pomieszczeniach o ograniczonym i kontrolowanym dostępie.

Zagrożenia komunikacyjne (sieciowe). Podczas przesyłania danych kanałem komunikacyjnym należy mieć na uwadze fakt, że mogą zostać one przechwycone przez fizyczne wpięcie się osób niepowołanych w sieć lub poprzez programy podsłuchujące transmisję. Dlatego wszystkie ważne dane powinny być szyfrowane z użyciem silnych metod kryptograficznych.

Istnieje tutaj metoda ochrony systemu teleinformatycznego przed posłuchem lub dostępem do systemu informatycznego wraz z jego zasobami.

Zagrożenia związane z oprogramowaniem. Każde oprogramowanie posiada błędy i luki, które poprzez aktualizację są naprawiane. Jeśli chodzi o oprogramowanie stosowane w systemach teleinformatycznych, powinno się jak najczęściej aktualizować oprogramowanie użytkowe i antywirusowe do najnowszej wersji. Należy również zwrócić uwagę na złośliwe oprogramowania typu exploity, wirusy, trojany itp.

Zagrożenia związane z inżynierią społeczną. Najlepsze jednak zabezpieczenia i najbardziej wyszkoleni administratorzy systemu są bezradni, jeśli użytkownikami są osoby lekkomyślne. Znajdują tutaj zastosowanie metody socjotechni-

ki, które polegają na uzyskaniu informacji niejawnych poprzez stosowane specjalnie do tego celu środki, np. podszywanie się pod innych użytkowników, przekupstwo czy metoda *dumpster diving*. Ponadto głównym błędem użytkowników jest zabezpieczanie systemu za pomocą prostych haseł łatwych lub stosowanie tych samych haseł do wielu elementów systemu czy zapisywanie haseł w ogólnodostępnym miejscu, np. na biurku lub monitorze.

Poza wskazanymi powyżej głównymi zagrożeniami należy zwrócić uwagę na czynniki mające wpływ na bezpieczeństwo pracowni komputerowej, takie jak: kradzież sprzętu komputerowego, utrata możliwości korzystania z łączy telekomunikacyjnych, niedomaganie administratora, brak dostępu do części zapasowych w serwisie.

**Zagrożenia w pracowni komputerowej**

Badania własne dotyczące funkcjonowania i bezpieczeństwa informatycznego wydziałowych pracowni komputerowych wskazały, że spośród różnych typów zakładanych zagrożeń, jak: fizyczne uszkodzenia podzespołów komputera, brak zasilania, awaria urządzeń teleinformatycznych, uszkodzenie/zniszczenie gniazd wejścia/wyjścia, niesprawność systemu operacyjnego, niedziałające/ niewłaściwie funkcjonujące oprogramowanie użytkowe, kradzież elementów zestawu komputerowego, nieuprawniony/nieautoryzowany dostęp do oprogramowania, nadużycie/fałszowanie praw dostępu, najczęściej występującym zagrożeniem jest awaria urządzeń teleinformatycznych oraz niesprawność systemu operacyjnego. Awarie sprzętowe występują sporadycznie i te wymagają bardzo często działań serwisu lub dostawcy usług internetowych. Przyczyny zaistnienia uszkodzeń lub problemów związanych z oprogramowaniem komputerów są różne. Mogą to być uszkodzenia wywołane przez użytkowników, wirusy komputerowe, nieuprawniony dostęp. Wobec powyższego priorytetowym zadaniem staje się zapewnienie niezawodności działania pracowni komputerowej poprzez sprawne przywrócenie systemu operacyjnego i zainstalowanych programów użytkowych na poszczególnym zestawie komputerowym.

**Możliwości rozwiązań**

Głównym celem projektowania systemu bezpieczeństwa pracowni komputerowej jest jednak minimalizowanie strat wywołanych naruszeniem zasad dostępu lub procedur bezpieczeństwa. Dostępne powszechnie metody i formy przeciwdziałania zagrożeniom, np. kopie bezpieczeństwa, fizyczne i wirtualne nośniki danych, oraz nowe technologie, jak deduplikacja, ciągła ochrona danych (CDP), przechowywanie danych w chmurze czy skorzystanie z usług dotyczących przechowywania plików w sieci (np. Google Drive, SugarSync, Dropbox, Box, Insync, Cubby), związane są z pewnymi kosztami.

Na rynku dostępne są profesjonalne programy do archiwizacji, automatycznego tworzenia kopii zapasowych i odzyskiwania danych. Istnieje jednak wiele dostępnych programów dla użytkowników prywatnych (domowych) chcących archiwizować dane bądź tworzyć kopie zapasowe. Są to oprogramowania darmowe lub proponowane użytkownikom wersje testowe na około 30 dni (EASEUS Todo Backup, AOMEI Backupper, HDClone Free Edition, Cobian Backup, Abakt, FBackup, Abelssoft Backup, Acronis True Image itp.).

Najczęściej występujący w pracowniach system operacyjny Windows udostępnia kilka narzędzi do wykonania kopii zapasowej. Są to: kopia zapasowa plików, kopia zapasowa obrazu systemu, poprzednia wersja, przywracanie systemu, jednak narzędzia te nie zapewniają 100-procentowego bezpieczeństwa.

**Wykorzystanie programu Clonezilla**

Wobec powstawania uszkodzeń lub problemów związanych z oprogramowaniem komputerów w pracowni komputerowej dla zapewnienia ciągłości procesu dydaktycznego zadaniem staje się sprawne przywrócenie systemu operacyjnego i zainstalowanych programów użytkowych na poszczególnych komputerach. Taką szansę stwarza darmowy program Clenzilla. Jest to bootowalny system operacyjny GNU/Linux obsługujący formaty plików: ext2, ext3, ext4, reiserfs, reiser4, xfs, jfs dla GNU/Linux, FAT, NTFS dla Windows, HFS+ dla Mac OS, UFS dla FreeBSD, NetBSD, OpenBSD, VMFS i VMWare dla ESX. Dlatego za pomocą Clonezilla można wykonać kopię zapasową partycji oraz dysków (*backup*) i przywrócić (*restore*) system GNU/Linux, MS Windows, Mac OS, FreeBSD, NetBSD, OpenBSD, Minix i VMWare ESX bez względu na to, czy jest to 32-bitowy (x86), czy 64-bitowy (x86-64) system operacyjny. Dostępne są Clonezilla live dla stacji roboczej i Clonezilla SE (server edition).

Program wewnętrznie korzysta z 3 narzędzi: partclone, partimage oraz dd. Zapisuje obraz partycji w formie pliku do wskazanego przez użytkownika folderu i pozwala również odtworzyć obraz, wymaga jednak znajomości poszczególnych funkcji, jest nieco skomplikowany dla niedoświadczonego użytkownika oraz posiada pewne ograniczenia. Program Clonezilla może być uruchomiony z płyty CD, pamięci flash USB lub dysku twardego USB. Minusem programu jest brak prostego interfejsu oraz ograniczone wersje językowe, brak możliwości przywracania obrazu partycji większej na mniejszą partycję docelową.

W odniesieniu do pracowni komputerowej wykorzystanie programu Clonezilla i zakres postępowania przy tworzeniu obrazu dysku sprawia pewną trudność, wymaga bowiem podstawowej znajomości języka programu, wykonania całej procedury tworzenia obrazu oraz przywracania wobec każdej jednostki, co wymaga nakładu czasu i pracy. Ponadto zapisanie obrazu partycji do pliku łączy się z niebezpieczeństwem jego usunięcia celowo lub przypadkiem.

Program jednak po napisaniu odpowiedniej aplikacji daje możliwość niezawodnego i szybkiego przywracanie systemu oraz uniemożliwia dostęp z poziomu systemu Windows. Autorzy artykułu udostępniają zainteresowanym osobom lub szkołom stworzoną aplikację[1].

## Opis działania aplikacji

Najpierw instalując system Windows oraz oprogramowanie użytkowe, należy zarezerwować odpowiednią ilość miejsca na dysku twardym nieprzydzieloną do żadnej partycji. Następnie z wykorzystaniem aplikacji zostaje przydzielone całe wolne miejsce na nową partycję, a po sformatowaniu zainstalowany tam system Clonezilla. Wszystkie funkcje oprócz przywrócenia partycji zostały zabezpieczone hasłem. Przy bootowaniu z twardego dysku są tylko dwie opcje wyboru systemu Windows lub Clonazilla. Uruchamiając Clonezilla, można wykonać *backup* partycji windowsowej poprzez wybór odpowiedniej opcji lub ją przywrócić w miarę szybko. Nazwa obrazu kopii zapasowej jest tworzona na podstawie aktualnej daty na komputerze. Wybranie i potwierdzenie obrazu do przywrócenia automatycznie rozpoczyna proces przywracania systemu. Mogą to uczynić nauczyciele lub sami uczniowie przed rozpoczęciem zajęć lub w przypadku stwierdzenia niesprawności działania systemu operacyjnego. Aplikacja uniemożliwia pozostawienie na komputerze nieautoryzowanych lub nielegalnych programów użytkowych, wirusów lub złośliwego oprogramowania. Ponadto jest oparta na ogólnie dostępnym oprogramowaniu linuksowym.

## Podsumowanie

Zapewnienie niezawodności działania oraz bezpieczeństwa systemów operacyjnych jest trudnym i ważnym zagadnieniem informatyki. Przedstawione rozwiązanie stanowi jedną z prób rozwiązania problemu, jakim jest zapewnianie niezawodności i bezpieczeństwa systemów komputerowych w pracowni komputerowej. Umożliwia automatyczne przywracanie partycji systemowej przez dowolnego użytkownika w miarę potrzeb, całkowicie eliminując możliwość modyfikacji przez nieuprawnioną osobę. Ponadto wykonany program jest skuteczny, efektywny, tani oraz prosty do wdrożenia. Jedynym ograniczeniem przedstawionego rozwiązania może być fizyczne uszkodzenie dysku twardego lub istotnych podzespołów komputera.

## Literatura

*Bezpieczeństwo komputerowe szkoły. Poradnik* (2016). Warszawa: UKE.
Laskowski, M. (2013). *Bezpieczeństwo systemów informatycznych*. Lublin: Wyd. PL.

[1] Aplikacja udostępniana przez autorów artykułu w polskiej wersji językowej: m.sniadkowski@pollub.pl.