

Paweł Szeliga, Mariusz Nycz

Niskobudżetowa platforma ochrony danych

Edukacja - Technika - Informatyka nr 4(18), 339-344

2016

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.



PAWEŁ SZELIGA¹, MARIUSZ NYCZ²

Niskobudżetowa platforma ochrony danych

Low-budget platform of data protection

¹ Inżynier, Politechnika Rzeszowska im. Ignacego Łukasiewicza, Polska

² Doktor inżynier, Politechnika Rzeszowska im. Ignacego Łukasiewicza, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, Polska

Streszczenie

Artykuł jest adresowany w głównej mierze do użytkowników domowych, jak i mikrofirm. Praca rozpoczyna się od przedstawienia problemu, jakim jest ciągły przyrost generowanych danych. W dalszej części rozdziału autorzy prezentują główne przyczyny utraty danych oraz określają częstotliwość wykonywania kopii zapasowej w sieciach domowych. Następnie omówiona zostaje sprzętowa platforma Raspberry, która została wykorzystana do zaimplementowania mechanizmów tworzących technologie sieciowych dysków NAS w sieci domowej.

Słowa kluczowe: Raspberry Pi, Network Attached Storage, kopia zapasowa, ochrona, dysk NAS.

Abstract

The article is addressed primarily to home users and micro businesses. The work begins with the presentation of the problem, which is the continuous growth of data generated. In the next section the authors present the main causes of data loss and determine the frequency of the backup in home networks. Then discussed is the hardware platform Raspberry, which was used to implement the mechanisms of creating technologies of network NAS drive on your home network.

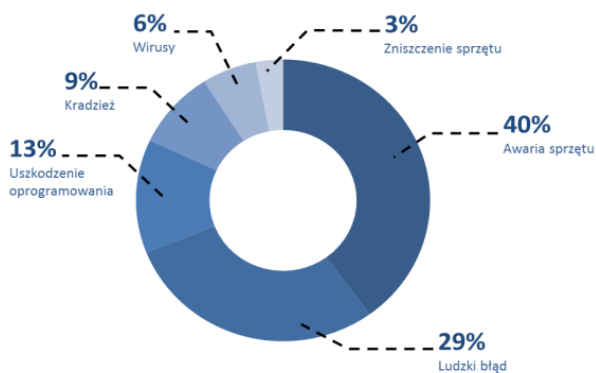
Key words: Raspberry Pi, Network Attached Storage, backup, protection, NAS.

Wstęp

Rozwój coraz to nowszych technologii wpływa nie tylko na rozwój gospodarki, ale także dotyczy wszystkich dziedzin życia. Z każdym rokiem coraz większą wagę przykłada się do odpowiedniego zabezpieczenia danych. Duża ilość informacji przechowywana jest w chmurach lub na dyskach serwerowych. Niestety rozwiązania tego typu nie są do końca bezpieczne. W większości przypadków, gdy zdecydujemy się na korzystanie z chmury publicznej, zrzekamy się praw do przechowywanych danych. Z punktu prawnego oznacza to, iż nasze dane należą do właściciela chmury. Inaczej wygląda sytuacja w przypadku da-

nych przechowywanych w chmurze prywatnej, gdzie dane zawsze będą należeć do użytkownika. Niezależnie od wykorzystywanej chmury pojawia się problem odpowiedniego zabezpieczenia danych przed nieautoryzowanym dostępem osób trzecich.

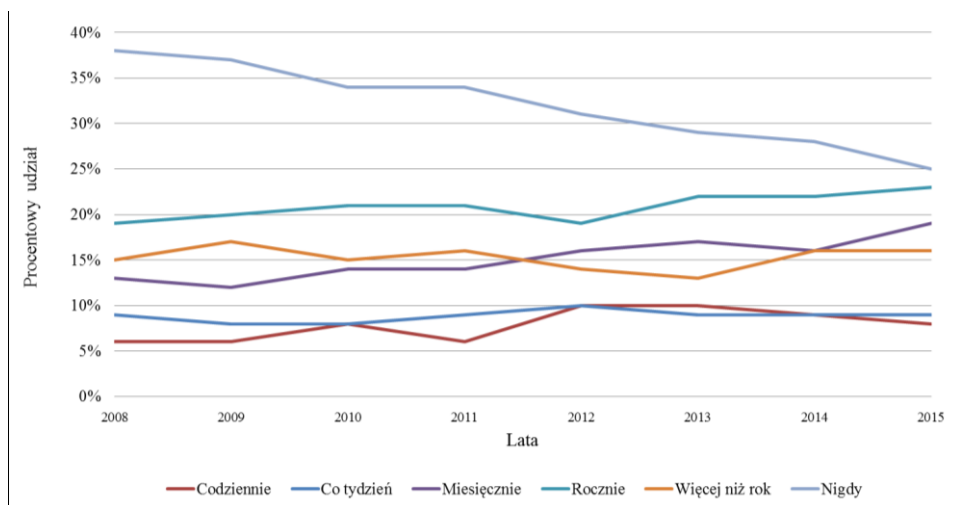
Jak podają statystyki, ludzie codziennie generują 2,5 trylionów bajtów danych [Walker]. Dla porównania, 90% danych generowanych w ciągu jednego dnia zostało wygenerowanych w ciągu ostatnich 2 lat. W roku 1992 wszyscy użytkownicy byli w stanie wygenerować zaledwie 100 Gb danych w ciągu dnia, natomiast w roku 2013 liczba generowanych danych wzrosła do 28,875 Gb w ciągu sekundy. Jak wspomnieliśmy wcześniej, odpowiednie zabezpieczenie danych jest bardzo trudne. Jednym z głównych powodów przechowywania danych w chmurach jest wykonanie kopii zapasowej plików. Przyczyny utraty danych są rozmaite, począwszy od fizycznego uszkodzenia dysku, aż do zaszyfrowania nośnika za pomocą złośliwego oprogramowania. Wykres 1 prezentuje najczęściej występujące przyczyny utraty prywatnych danych [Safebackup].



Wykres 1. Główne przyczyny utraty danych

Źródło: [Safebackup].

Na każdym z komputerów są przechowywane takie dane, których użytkownik nie powinien stracić. W przypadku komputerów prywatnych są to zdjęcia, dokumenty czy prywatne pliki, natomiast w przypadku firm są to umowy, rozliczenia, raporty, faktury czy też inne dokumenty. W każdym z tych przypadków starta danych jest punktem krytycznym. Niekiedy odzyskanie danych jest procesem bardzo kosztownym i długotrwałym. Zdarzają się przypadki, w których odzyskanie danych jest niemożliwe. Większość z ludzi nie pamięta o regularnym wykonywaniu kopii zapasowej. Wykres 2 przedstawia częstotliwość wykonywania kopii w latach 2008–2015. Statystyki dotyczą użytkowników domowych [Klein].



Wykres 2. Częstotliwość wykonywania kopii zapasowej w latach 2008–2015

Źródło: [Klein].

Platforma Raspberry Pi

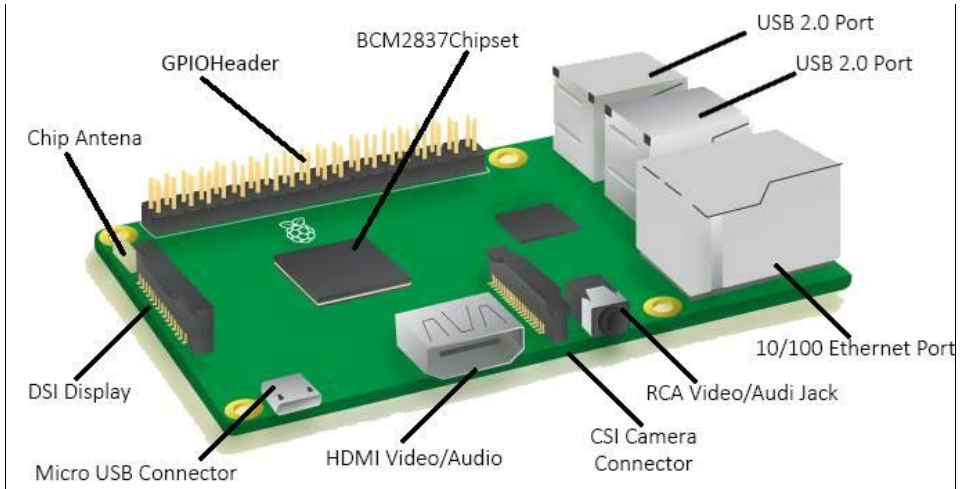
Raspberry Pi jest to minikomputer opracowany przez Raspberry Pi Foundation, natomiast zaprojektowany na Uniwersytecie Cambriach. Pierwsze modele sprzętowej platformy powstały w roku 2012. Liczba zastosowań dla minikomputera ciągle wzrasta. Urządzenie to można wykorzystać jako platformę do nauki programowania, domowe centrum rozrywki czy też komputer z zainstalowanym systemem Linux bądź Windows. Do tej pory stworzono 6 modeli Raspberry Pi, z których najnowszy jest Raspberry Pi 3. Jego premiera odbyła się 29 lutego 2016 r. W tabeli 1 przedstawiono charakterystykę podstawowych parametrów dla wybranych modeli.

Tabela 1. Charakterystyka podstawowych parametrów najpopularniejszych modeli Raspberry Pi

	Raspberry Pi B+	Raspberry Pi 2 B	Raspberry Pi 3 B
Procesor	700 MHz ARMv6 Single Core	900 MHz ARMv7 Quad Core	1 GHz ARM Cortex-A53 64 Bit Quad Core
Pamięć RAM	512 MB	1 GB DDR2	1GB DDR2
USB	4	4	4
Połączenia sieciowe	Ethernet 100 Mbit	Ethernet 100 Mbit	Ethernet 100 Mbit Wi-Fi 2.4 GHz Bluetooth
Zasilanie	600 mA	900 mA	2.5 A

Źródło: [Bates 2015: 14–21].

Najnowszy model minikomputera został wyposażony w moduł Bluetooth oraz moduł wi-fi, dzięki czemu możliwości wykorzystania urządzenia znacząco wzrosły. Ponadto wersja 3 jest dużo bardziej wydajna w stosunku do swoich poprzedników [Bates 2015: 1–8]. Rysunek 1 przedstawia architekturę najnowszej platformy Raspberry Pi.



Rys. 1. Architektura Raspberry Pi 3

Architektura płytki umożliwia rozbudowę minikomputera o wysokiej rozdzielczości kamerę, dysk WDPiDrive o pojemności 1TB czy też specjalnie przygotowany wyświetlacz. Cena urządzenia bez wyżej wymienionych akcesoriów w dniu premiery wynosiła tylko 220 zł.

Raspberry Pi 3 jako Network Attached Storage

Technologia Network Attached Storage umożliwia podłączenie zasobów pamięci dyskowych do sieci komputerowej. Niezbędnymi elementami serwera NAS jest kontroler oraz dysk, gdzie role kontrolera będzie pełnił urządzenie Raspberry z zewnętrznym dyskiem zasilanym z portem USB. Istnieje też możliwość zakupu specjalnego dysku WDPiDriver. Dyski NAS wykorzystywane są w głównej mierze do wykonywania kopii zapasowych plików [Bruce 2015: 1–6]. Użytkownicy, którzy potrzebują bezpiecznie przechowywać swoje zdjęcia, muzykę, dokumentacje projektów, materiały naukowe czy umowy, powinni zastanowić się, w jaki sposób mogą zautomatyzować wykonywanie kopii zapasowej [Sohan 2015: 1]. Autorzy przedstawiają rozwiązanie kierowane głównie dla użytkowników domowych bądź też mikrofirm, którego zadaniem będzie wykonywanie w sposób zautomatyzowany kopii zapasowych. Cały projekt wykonywany był w sieci LAN [Princy 2015: 1–2].

Pierwszy etap tworzenia środowiska automatycznego wykonywania kopii zapasowych wymaga instalacji systemu operacyjnego dla urządzenia Raspberry Pi. Istnieje kilka dedykowanych środowisk dla tego urządzenia. W przedstawionej konfiguracji został wykorzystany dostępny na stronie producenta obraz instalacyjny Noobs. Umożliwia on zainstalowanie Raspbiana – podstawowego systemu operacyjnego. Pierwszym krokiem zainstalowanego systemu powinno być skonfigurowanie statycznego adresu urządzenia, za pomocą którego użytkownik będzie wstanie połączyć się zdalnie, wykorzystując do tego celu oprogramowanie putty czy też zdalny pulpit. Przed wykonaniem czynności mających na celu automatyczne wykrywanie dysku należy przeprowadzić aktualizację oprogramowania oraz aktualizację pakietów znalezionych w repozytoriach. Do tego celu zostaną wykorzystane polecenia *sudo apt-get update* oraz *sudo apt-get upgrade*. Po wykonaniu powyższych czynności należy podłączyć dysk, który ma pełnić funkcję dysku sieciowego. W kolejnym kroku konfiguracji należy zamontować dysk w stworzonym katalogu. Można tego dokonać, wykorzystując polecenie *mount*. Aby nie trzeba było powtarzać czynności montowania dysku po każdym uruchomieniu pliku należy zmodyfikować plik */etc/fstab* poprzez dodanie na końcu pliku linii */dev/sda1 /media/Dysk_NAS auto defaults 0 2*, gdzie *sda1* jest identyfikatorem dysku, a lokalizacja */media/Dysk_NAS* jest lokalizacją, w której ma zostać zamontowany dysk. Po wykonaniu tej czynności należy uruchomić urządzenie Raspberry ponownie.

Jak widać, dysk od tej pory montowany jest automatycznie, dlatego też pozostało go udostępnić dla użytkowników sieci. Do tego celu zostanie wykorzystany pakiet *samba*. Instalacja przebiega dokładnie w taki sam sposób, jak w przypadku środowisk linuksowych. Aby udostępnić lokalizację dysku należy zainstalować także pakiet *samba-common-bin*. W tym momencie należy przeprowadzić konfigurację wcześniej zainstalowanych pakietów. Proces ten zostanie przeprowadzony w pliku konfiguracyjnym *smb.conf*. Na końcu pliku należy dodać sekcję odpowiadającą za konfigurację dysku sieciowego. Konfiguracja ta została przedstawiona na rys. 2.

```
[Dysk_NAS]
path = /media/Dysk_NAS
comment=Dysk udostepniony
force group = users
valid users = @users
writeable = yes
browseable = yes
read only = no
public = yes
directory mask = 0777
create mask = 0777
```

Rys. 2. Konfiguracja odpowiadająca za udostępnienie dysku w sieci LAN

W tym momencie należy uruchomić ponownie usługę samby. Po wykonaniu wszystkich czynności użytkownik powinien zobaczyć w sieci udostępniony dysk o nazwie *Dysk_NAS*. W przypadku, gdy zachodzi potrzeba zabezpieczenia dysku, istnieje możliwość wprowadzenia uwierzytelniania [Reed 2000: 1–3]. Można dokonać tego za pomocą komendy `sudo smbpasswd -a pi`, po wykonaniu której użytkownik zostanie poproszony o podanie hasła dostępu dla użytkownika pi. Po ponownym uruchomieniu usług samby dysk zostanie zabezpieczony hasłem. Aby system działał bez ingerencji użytkownika, tzn. operacja wykonywania tzw. backupu była wykonywana automatycznie, należy stworzyć plik o rozszerzeniu bat zawierający polecenia kopiowania wraz z odpowiednimi parametrami i ścieżkami. Następnie należy dodać taki skrypt do harmonogramu zadań. Od tej pory wszystkie operacje kopiowania plików będą wykonywane w zależności od wprowadzonych ustawień w harmonogramie. Autorzy zalecają wykonywanie kopi zapasowych ważnych plików przynajmniej raz w ciągu tygodnia. Pozwoli to na zminimalizowanie strat podczas potencjalnej awarii dysku.

Podsumowanie

Autorzy zwracają uwagę na problem, jakim jest utrata ważnych danych. Niestety w przypadku niektórych uszkodzeń dysków nie jest możliwe odzyskanie danych. Użytkownicy niestety nie widzą konieczności przeprowadzania operacji backupu do momentu, kiedy nie zostaną zagrożone ich pliki. Bardzo często koszt odzyskania danych jest dużo większy niż koszt zaprezentowanego przez autorów domowego systemu do wykonywania kopi zapasowej. Ponadto platformę Raspberry można wykorzystać także do wielu innych projektów. Jest to ciekawe rozwiązanie umożliwiające wykonanie wielu projektów naprawdę niewielkim kosztem.

Literatura

- Bates D. (2015), *Raspberry Pi Projects for Kids*, Birmingham.
- Bruce R.F. (2015), *Make Space for the Pi*, SoutheastCon 2015, Fort Lauderdale.
- Klein A., *Welcome to Backup Awareness Month 2015*, <https://www.backblaze.com/blog/backup-awareness-month-2015/>.
- Princy S.E. (2015), *Implementation of Cloud Server for Real Time Data Storage Using Raspberry Pi*, Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore.
- Reed B.C. (2000), *Authenticating Network Attached Storage*, „IEEE Micro” vol. 20, issue 1.
- Safebackup, *7 Greatest Causes of Data Loss*, http://www.databackuponlinestorage.com/7_Causes_of_Data_Loss.
- Sohan R. (2005), *A User-level Approach to Network Attached Storage*, The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05), Sydney, NSW.
- Walker B., *Every Day Big Data Statistic*, <http://www.vcloudnews.com/every-day-big-data-statistics-2-5-quintillion-bytes-of-data-created-daily/>.