

## Cała prawda o Naszej Klasie

Czy zastanawialiście się co jest przyczyną tak szybkiego wzrostu popularności portalu, który od początku swego istnienia posiadał tak wiele wad? Czy korzystając z serwisu możemy czuć się bezpiecznie? Jeśli gnębią Was te pytania – koniecznie przeczytajcie artykuł.



A już w następnym numerze:

## Dyski SSD: krok, tylko w którą stronę?

Dyski SSD działają podobnie jak pamięci flash, czyli inaczej mówiąc, wykorzystują technologie pozwalające zapisywać i/lub kasować kilka komórek pamięci naraz. Czy zaspokoją zapotrzebowania nawet najbardziej wybrednych klientów? Przeczytaj, aby dowiedzieć się więcej.

**Bezpieczeństwo**  
Mądry Polak przed  
szkodą - archiwizacja  
danych



**Bezpieczeństwo**  
Kilka słów  
o zagrożeniach w sieci



Drodzy Czytelnicy,

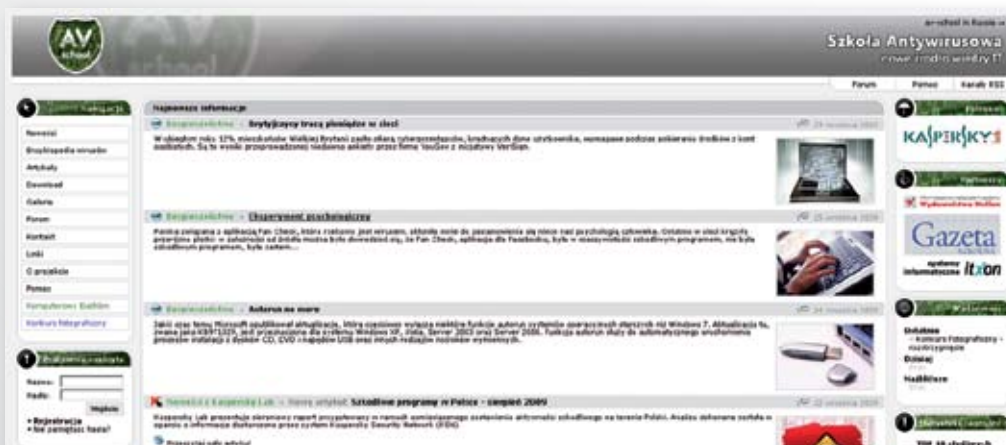
W oczach ludzi dorosłych, obecna młodzież coraz częściej rysuje się jako pokolenie nieambitne, bez szacunku do nauki, niezainteresowane światem. Na szczęście obraz ten nie do końca jest prawdziwy. Na dowód tego, przedstawiamy Wam magazyn „Stricte”, gazetkę wydawaną przez ludzi młodych. Stricte, jak zapewne każdy wie, oznacza „ściśły, precyzyjny, dokładny”. Wiedza wymaga przecież dokładności, bo czym byłaby, gdybyśmy pozostawiali ją w zarysach? Trzeba ją zgłębiać i rozpowszechniać – to właśnie jest naszym celem. Wierzymy zatem, że będziemy w stanie przybliżyć świat naszych pasji każdemu Czytelnikowi.

Zespół redakcyjny stanowi grupa uczniów, którzy zostali wybrani przez portal AV-School. Osoby te wyróżniały się w konkursach czy w życiu serwisu. Dostaliśmy szansę i jak sami widzicie, nie marnujemy jej. Mamy nadzieję, że lektura „Stricte” sprawi Wam przyjemność i satysfakcję.

Zespół redakcyjny „Stricte”

AV-School.pl to:

- źródło informacji z dziedziny IT
- konkursy z atrakcyjnymi nagrodami
- możliwość zaprezentowania swoich umiejętności
- nauka poprzez zabawę
- moderowane forum
- pozytywne emocje



**Zespół redakcyjny:**

**Redaktor Naczelny:** Krzysztof Parkitny

**Redaktorzy:** Katarzyna Adamek, Damian Raksimowicz, Jakub Pierzchała, Patrycja Dziubek, Dawid Leśniak, Jakub Sobczyk

# Z życia AV – School

*Autor: Katarzyna Adamek*

Na początek kilka słów „o nas”. Portal AV-School.pl ma na celu szerzenie wiedzy o bezpiecznym korzystaniu z Internetu oraz komputera. Projekt daje możliwość poszerzania swojego informatycznego doświadczenia. Na bieżąco pojawiają się tam artykuły o najnowszych zagrożeniach. Każdy ma możliwość stać się członkiem informatycznej społeczności, połączonej wspólnymi poglądami.

## Konkursy, konkursy, konkursy...

Mimo, że miesiące letnie są uważane za czas wypoczynku, portal AV-School.pl tętni życiem. 10 czerwca zakończył się Komputerowy Biathlon. Konkurs składał się z 6 etapów, z którymi uczestnicy zmagali się przez 6 tygodni. Do konkursu zgłosiło się 285 drużyn z gimnazjów i szkół średnich z całej Polski.

I miejsce oraz III miejsce zajęły drużyny „Chabior Team” i „White Group” z Zespołu Szkół Elektronicznych i Informatycznych w Sosnowcu, nad którymi opiekę sprawowała Pani Profesor Irena Sowińska. II miejsce przypadło drużynie „zamoyfighters” z V LO im. Kanclerza Jana Zamoyskiego w Dąbrowie Górniczej. Opiekunem uczniów był Pan Profesor Marcin Kosior.

Dodatkowo organizatorzy postanowili przyznać Nagrodę Specjalną dla najlepszej drużyny gimnazjalnej. Nagrodę otrzymała drużyna „hands in future” z Publicznego Gimnazjum nr 2 w Chrzanowie. Opiekę nad drużyną sprawowała Pani Małgorzata Pawlik.

Zwycięzcy otrzymali pakiet programów Kaspersky Internet Security 2009 oraz Acronis True Image 11. Ponadto szkoła reprezentowana przez

zwycięską drużynę, otrzymała oprogramowanie Kaspersky Work Space Security (pracownia komputerowa). Zespoły z miejsc II i III oraz wyróżniona drużyna gimnazjalna otrzymały nagrody niespodzianki. Ponadto wszystkie wymienione drużyny zostały uhonorowane dyplomami i gadżetami Polskiego Związku Biathlonu.

28 sierpnia zakończył się letni Konkurs Fotograficzny. Zdjęcia, nadesłane przez Uczestników przedstawiały wakacyjne motywy, ale dodatkowo... musiał znaleźć się na nich komputer. Użytkownicy, którym kreatywność nie była obca, niemal przez całe wakacje nadsyłali swoje zdjęcia. Nie wszystkie fotografie zakwalifikowały się do ścisłego finału, ze względu na tematykę odbiegającą od zamierzonej. Ostatecznie zwycięzcą został Mikołaj Neckar z Wrocławia, otrzymując w nagrodę iPod'a!



Wiemy, że to nie ostatni konkurs organizowany przez AV-School. Po udanej pierwszej edycji Komputerowego Biathlonu, liczymy na kolejne konkursy informatyczne.

W najbliższym czasie planowany jest Konkurs dla Programistów, w którym uczestnicy będą mogli zaprezentować w praktyce swoje umiejętności. Jesień to również czas na ogłoszenie kolejnej edycji Komputerowego Biathlonu. Uczniowie, jak również szkoły sprawujące nad nimi opiekę po raz kolejny będą mieć szansę na zdobycie atrakcyjnych nagród. Zapraszamy do rywalizacji!

Zaglątajcie na stronę: [www.av-school.pl](http://www.av-school.pl), gdzie znajdują się najświeższe informacje z życia portalu.

# Cała prawda o naszej-klasie

Autor: *Jakub Pierzchała*

Zapewne większość z Was słyszała, bądź miała styczność z Naszą Klasą – jednym z największych polskich serwisów społecznościowych. Czy jednak zastanawialiście się co jest przyczyną tak szybkiego wzrostu popularności portalu, który z początku swego istnienia posiadał wiele wad? Czy korzystając z serwisu możemy czuć się bezpiecznie? Jeśli gnębią Was te pytania – koniecznie przeczytajcie artykuł.

## Jak to się zaczęło?

Nasza-Klasa została utworzona w 2006 roku przez czterech studentów informatyki z Wrocławia. Początkowo, głównym założeniem serwisu było umożliwienie użytkownikom odnalezienia swoich dawnych znajomych, szkół i klas, do których

nie istnieje możliwość dołączenia do różnego rodzaju grup, lub klubów łączących osoby mające podobne poglądy i zainteresowania. Innym powodem, dla którego Nasza-Klasa przyciąga rzesze ludzi jest fakt, że z łatwością możemy w niej wyidealizować samych siebie, wzbudzając zazdrość w naszych rówieśnikach, ale o tym niżej.

## Autokreacja - czyli jak chcemy być postrzegani

Co jeszcze przyciąga nas do Naszej-Klasy? Oczywiście możliwość pochwalenia się przed szerokim gronem naszymi dokonaniem. Wszyscy z przyjemnością dodają zdjęcia z egzotycznych, drogich wycieczek, zdjęcia dobytku swojego życia, swo-



uczyszczali. Pomimo sporej niestabilności i ciągłego widoku Pana Gąbki, do „NK” zaczęło przyłączać się coraz więcej Internautów. Dlaczego akurat Nasza-Klasa, a nie inne portale społecznościowe zdobyła w Polsce tak wielką popularność? Istnieje wiele różnych powodów. Jeden z ważniejszych wskazują psychologowie i socjologowie. Ich zdaniem, przeciętny użytkownik chce udowodnić sobie i innym, że jest połączony z konkretną grupą osób, z którymi łączy wspólne wspomnienia i doświadczenia. Nasza-Klasa potrafi zaspokoić tę potrzebę, pozwalając nam przyłączyć się do konkretnego grona. Początkowo mogliśmy przyłączyć nasz profil do naszej bylej klasy, bądź szkoły. Obec-

nie domy lub mieszkania, samochody i oczywiście kochane pociechy. Do pewnego momentu jest to jak najbardziej normalne. Przecież nie poświęcamy się ciężkiej pracy, by później ukrywać wszystkie nabyte dzięki niej korzyści. Jednak coraz częściej możemy spotkać się z ludźmi, którzy na siłę próbują się wywyższyć. Umieszczają oni zmontowane zdjęcia, podają nieprawidłowe dane, a nawet zapisują się do szkół, w których nigdy się nie kształcili. Znajdują się też tacy, którzy potrafią dodawać do swoich znajomych całkowicie nieznane im osoby, po to tylko, by każdy mógł zobaczyć ilu mają znajomych. Powód takiego zachowania jest jeden – użytkownik koniecznie chce podnieść swoją war-

tość w oczach innych. Oczywiście możliwość wyidealizowania samego siebie może przyciągać, jakkolwiek należy pamiętać, że wszyscy jesteśmy ludźmi i takie rzeczy najczęściej prowadzą do najwzklejszej zazdrości, co można zaobserwować w komentarzach do zdjęć i profili. Lecz zastanówmy się, czy to właśnie po to powstała Nasza-Klasa...

## Czy jesteśmy bezpieczni?

Jak sugerują media, Nasza-Klasa stanowi drugą co do wielkości bazę danych osobowych w Polsce (pierwsze miejsce zajmuje TP SA). Każdy zarejestrowany użytkownik, ma dostęp do wielu informacji. O ile nie powinno to stanowić problemu w przypadku, gdy nasze dane zobaczą zaufane osoby, o tyle cyberprzestępcy z łatwością będą mogli uprzykrzyć nam życie. Manipulacją, szantażem, bądź innymi metodami, mogą również próbować wymusić na nas przelew naszych pieniędzy na ich konta. Swego czasu głośno było o Internaucie, który stworzył fikcyjne konto znanej piosenkarki. Wysłał z niego wiadomości do innych użytkowników, z prośbą o pomoc finansową w leczeniu swojego ciężko chorego dziecka. Na szczęście oszustwo wyszło na jaw, lecz musimy pamiętać, że takie insynuacje się zdarzają. Okazuje się, że „NK” może też być i jest, skutecznie wykorzystywana przez różnego rodzaju firmy bądź instytucje wykorzystujące dane osobowe. Nie stanowi to może dużego niebezpieczeństwa, jak w przypadku cyberprzestępców, ale powinniśmy być świadomi tego faktu.

## A wystarczy trochę zdrowego rozsądku

Jeżeli chcemy ochronić informacje o nas przed niepożądanym wykorzystaniem, musimy pamiętać o paru ważnych sprawach. Po pierwsze, zapoznajmy się dokładnie z treścią regulaminu. Akceptując go, zgadzamy się na umieszczenie w serwisie naszych danych. Po drugie należy poważnie zastanowić się, które informacje chcemy udostępnić, a które zachować dla siebie.

Musimy również pamiętać, abyśmy sami nie stali się powodem proble-

mów. Dotyczy to szczególnie umieszczenia na naszym profilu grupowych zdjęć. Nieważne czy przedstawiają nas przy ognisku, czy w innych sytuacjach. Ważne żeby wszystkie osoby znajdujące się na fotografii, wyraziły zgodę na jej umieszczenie na portalu.

Przed wyborem „fotki”, którą chcemy umieścić w serwisie, naprawdę warto się zastanowić. W mediach głośno było o aferze, w której sześciu kontrwywiadowców umieściło w serwisie swoje zdjęcia z misji w Afganistanie. Dane osób pracujących w kontrwywiadzie są tak tajne, że nawet żołnierze z tego samego kontyngentu nie mają do nich dostępu. Nasza szóstka chyba o tym zapomniała, narażając na niepowodzenie całą operację. Mając przed oczami tę komiczną sytuację,

pomyślmy chwilę zanim umieścimy w naszej galerii.

### Co dalej z naszą –klasą?

Ze stwierdzeniem, że Nasza-Klasa odniosła spektakularny sukces, zgodzi się większość z nas. Uważam również, że wszyscy potwierdzą fakt, że nic nie trwa wiecznie. Zastanówmy się więc, co czeka tak popularny serwis w przyszłości. Jak wiemy głównym założeniem „NK”, było umożliwienie odnowienia kontaktów z przeszłości. Co jednak z użytkownikami, którzy już odnaleźli poszukiwane osoby, wymienili z nimi kontakty, bądź się ze sobą spotkali - zapewne z biegiem czasu coraz rzadziej będą odwiedzali serwis. Wybiorą inną formę komunikacji z dawnymi zna-

jomymi. Bez względu, czy będzie to telefon, czy e-mail, coraz mniej osób będzie używać w tym celu Naszej-Klasy. Do czego może to doprowadzić? Przede wszystkim, nieużywane konta będą zalegały w serwisie w coraz większych ilościach. Z pewnością nie zniszczy to serwisu, ale może delikatnie zachwiać jego fundamentami. Cóż, w rzeczywistości nikt nie może mieć stuprocentowej pewności, co będzie dalej. Jednym słowem pozujemy – zobaczymy.

Podsumowując – Nasza klasa może być świetnym narzędziem do podtrzymywania kontaktów. Wszystko leży jednak w naszych rękach i zależy od tego, jak będziemy uważać na swoje bezpieczeństwo, a także, w jaki sposób będziemy używać serwisu.

## Mądry Polak przed szkodą – archiwizacja danych

*Autor: Krzysztof Parkitny*

Komputer, oprócz codziennego centrum rozrywki i źródła informacji, stał się narzędziem ułatwiającym życie – co do tego nikt chyba nie ma wątpliwości. Ludzie przestają zapisywać daty wizyt u lekarza, numery telefonów czy adresów zamieszkania znajomych w notesach. Po co szukać długopisu i kawałka kartki gdzieś w szufladzie, skoro za pomocą kliknięcia myszy szybko i czytelnie można zapisać żądaną informację np. w systemowym notatniku? Jestem przekonany, że w tym momencie zastanawiasz się, jakiego typu informacje przechowujesz na dysku swojego komputera i jak bardzo są one ważne. Zastanów się więc również, co byś zrobił, gdyby wszystkie te dane nagle zniknęły?

### Czym jest archiwizacja danych?

Archiwizacja danych (*ang. backup*) to proces zabezpieczania danych poprzez tworzenie ich kopii. Choć w języku angielskim słowa archiving oraz backup to dwa różne określenia, to w naszym kraju przyjęło się, że „tworzenie backupu” to bardziej potoczne określenie archiwizacji danych. Archiwizacja jest nieodłącznym procesem wielu firm i korporacji, które przeznaczają na ten cel niemałe pieniądze. W takich firmach archiwi-

zacja jest dokonywana regularnie, co jest bardzo dobrym rozwiązaniem. Cały proces nie jest niczym trudnym, a elastyczność tworzenia kopii na różnych nośnikach jest olbrzymia.

### Po co tak naprawdę tworzyć kopie?

Mówiąc 'kopia danych' w prosty sposób można wyobrazić sobie pliki zapisane na innym nośniku niż dysk systemowy. Niestety, wciąż rzadko tworzymy kopie danych. Najczęściej myślimy o tym dopiero wtedy, gdy nasze dane zostały już uszkodzone. Bez wątplenia każdy kto znalazł się w takiej sytuacji, tracąc mniej lub bardziej ważne dane, wie o czym tutaj mowa. Nie będę przytaczał licznych przykładów z życia wziętych, w których prosta kopia danych mogła komuś oszczędzić wiele cennego czasu, nerwów, jak również pieniędzy. Przedstawię w prosty sposób proces archiwizacji danych, a Ty sam dokonasz wyboru czy jesteś „mądrym Polakiem przed szkodą”.

### Czym archiwizować?

Niewątpliwie pierwszym pytaniem, jakie należy sobie zadać jest kwestia, na jakiego typu nośniku chcemy archiwizować nasze dane. Warto pod-

kreślić, że niskim kosztem można zabezpieczyć się w sposób co najmniej odpowiedni. Poniżej krótkie przedstawienie najpopularniejszych możliwości archiwizacji danych.

1. Płyta CD/DVD –bardzo popularny nośnik danych. Z uwagi na fakt, że niemal w każdym komputerze znajduje się nagrywarka CD/DVD tworzenie kopii danych za pomocą tego urządzenia jest tanie. Nośniki CD/DVD kosztują od kilkudziesięciu groszy do kilku złotych w zależności od producenta i ich jakości. Minusem jest trwałość nośników, która pozostawia wiele do życzenia, zwłaszcza, jeśli płytę umieścimy w papierowym opakowaniu i pozostawimy w miejscu, gdzie jest podatna np. na naświetlanie.
2. Pamięć USB (potocznie pendrive, pamięć flash) – nośnik ten jest przede wszystkim bardzo poręczny, w wyniku czego częściej używany jest do przenoszenia danych niż do ich archiwizacji. Pamięci flash korzystające z interfejsu USB 2.0 uzyskują realną przepustowość do 40 MB/s, co można uznać za bardzo przyzwoity rezultat.
3. Dysk twardy – Prymitywnym nieco z uwagi na prostotę tworzenia

cd. na stronie 6

**BEZPIECZEŃSTWO**

backupu, zdaje się być wybór dysku twardego. Można tutaj przytoczyć dwa przypadki – dysk twardy podłączany za pomocą interfejsu USB, lub też dysk wbudowany wewnątrz jednostki centralnej (np. dyski ATA/SATA). Na korzyść tego rozwiązania przemawia cena, która nie jest wygórowana, jak również prostota i szybkość wykonania kopii (znana metoda 'przeciągnij-upuść'). Dostępne są dyski z funkcjami ułatwiającymi tworzenie kopii danych (najczęściej dyski USB). Ponadto producenci często dodają specjalistyczne oprogramowanie do takich celów, promując przy okazji swoje rozwiązania. Zdecydowanie odradza się jednak archiwizowanie danych na dysku systemowym. Procesu tego nie można uważać za tworzenie kopii zapasowej. Całość może mijać się z celem, gdyż w wyniku wypadku losowego (na przykład pożaru) ulec zniszczeniu może nie tylko dysk podstawowy, ale także dodatkowy, umieszczony praktycznie w tym samym miejscu. Poza tym, kopiując dane do innej lokalizacji na systemowy dysk twardy, zwiększamy ryzyko ich utraty, gdyż awaria dysku w wielu przypadkach sprawia, że wszystkie giną bezpowrotnie.

4. Napęd taśmowy (ang. streamer) – pojemny i niezawodny. Streamery używają jako nośnika danych taśm magnetycznych, które mają nawet do kilkuset gigabajtów pojemności. Wiele urzędów tego typu posiada różne ułatwienia, np. automatyczny backup. Mniej pozytywnym aspektem tego urządzenia jest cena, która rozpoczyna się od kilkuset, a kończy na tysiącach złotych. Głównie z tego powodu streamery stosowane są w korporacjach i firmach gdzie bezpieczeństwo danych jest niezbędne do działania całego przedsiębiorstwa i gdzie nie można oszczędzać na tak priorytetowych sprawach. Minusem tego rozwiązania jest również czas dostępu do danych – zarówno odczyt jak i zapis trwa stosunkowo długo.

Istnieje również tzw. archiwizacja 'on-line', o której przeczytasz w dalszej części artykułu.

### O czym należy pamiętać...

Praktycznie jedyne istotne pytanie, które należało sobie zadać, czyli wy-

bór nośnika, jest już za nami. Pora więc na kilka wskazówek, dzięki którym nasza praca (także po wykonaniu kopii zapasowej) nie pójdzie na marne. Oto one:

1. Nośników z kopią naszych danych nie przechowujemy blisko naszego komputera (oczywiście w miarę możliwości). Jeżeli, na przykład, nagramy płytę DVD z naszymi danymi, wkładamy ją do pudełka i umieszczamy je w biurku, na którym stoi nasza jednostka centralna. W tej sytuacji, jeżeli z różnych powodów nasz komputer zostanie zniszczony, najprawdopodobniej stracimy także nośniki z kopiami zapasowymi.



2. Archiwizacji danych należy dokonywać regularnie. Dzięki temu nowe dane pojawiające się na naszym komputerze także będą bezpieczne. Ponadto tworząc backup regularnie, łatwo można wyrobić sobie dobry nawyk.
3. Nośniki warto podpisywać – po co tracić czas i nerwy na szukanie odpowiedniego nośnika, na którym znajdziemy interesujące nas dane, skoro wszystko może być uporządkowane niemal zerowym nakładem pracy.
4. Nośników nie należy poddawać różnym czynnikom zmniejszającym ich żywotność. Chodzi tutaj głównie o bardzo wysokie lub niskie temperatury, czy miejsca gdzie mogą ulec fizycznemu uszkodzeniu.

### Druza strona medalu

Trzeba spojrzeć również na archiwizację z innej strony. Oczywiście, ideą całego procesu jest ogólnie mówiąc 'bezpieczeństwo danych', jednak tworząc backupy bez minimum wiedzy na ten temat sami powiększamy ryzyko utraty danych. Nie chodzi tu o ich fizyczną utratę lub zniszczenie, lecz o możliwość ich odczytania lub powielenia przez osoby niepowołane. W szczególności chodzi tutaj o tzw. 'archiwizację on-line', do której służą przeróżne portale (a właściwie

na chwile obecną serwisy społecznościowe) np. serwis odsiebie.com, który świadczy darmowe usługi hostingowe. Wielu ludzi używa tego portalu w celu podzielenia się swoimi plikami w sieci z kimś innym. Serwisy hostingowe służą jednak również (a niektóre – głównie) do archiwizacji danych, czyli poprzez 'uploadowanie' ich na serwer ftp/http, z którego w późniejszym czasie możemy ściągnąć nasze dane. Warto wtedy pamiętać, by odpowiednio je zabezpieczyć. Wysłanie swoich danych na jakiś inny, niedostępny dla nas fizycznie nośnik naraża je na to, że mogą zostać odczytane przez osoby trzecie. Rozwiązanie nie jest trudne. Wystarczy każdy plik, który wysyłamy na serwer zabezpieczyć silnym hasłem uniemożliwiając tym samym jego odczyt osobom niepowołanym. Służą do tego specjalne narzędzia. Można także posłużyć się prostym programem archiwizacyjnym typu WinZip. Jest to kolejna podstawowa zasada, tak oczywista, że wręcz niektórzy jej nie praktykują...

### Podsumowanie

W życiu codziennym myśląc o utracie danych zapisanych na naszym dysku tak naprawdę liczymy na szczęście – mamy nadzieję, że sprzęt nie zawiedzie. O fizyczne bezpieczeństwo swoich danych również jesteśmy spokojni, bo skoro korzystamy z komputera w domu, kto mógłby potrzebować naszych danych i w jakim celu? Najczęściej w takich przypadkach mówimy, że raczej nam się to nie przytrafi. Trzeba pamiętać jednak o czymś bardzo istotnym – mówiąc w ten sposób, nie polepszamy bezpieczeństwa swoich danych, co w gruncie rzeczy jest priorytetem podczas korzystania z komputera.

### CZY WIESZ, ŻE...

*Streamery stosowane są również w Policji. Są one najczęściej umieszczone w bagażnikach radiowozów policyjnych i zapisywane są na nich filmy z kamer policyjnych, przydatne np. podczas pościgów.*

*Silne hasło – hasło zbudowane z kombinacji wielu znaków, np. małe i duże litery, cyfry oraz znaki specjalne.*

# Kilka słów o zagrożeniach w Sieci

Autor: Damian Raksimowicz

Internet stał się dzisiaj podstawowym narzędziem napędzającym rozwój cywilizacyjny, społeczny i gospodarczy świata. Jego zastosowania – począwszy od poczty elektronicznej, transmisji danych, zdalnej pracy, handlu i transakcji elektronicznych do usług multimedialnych włącznie – stają się coraz bardziej powszechne, nie wspominając o użyteczności. Usługi szerokopasmowe, telefonia poprzez Internet i interaktywna telewizja zmieniają podstawowe zasady

olbrzymi wpływ na naukę i gospodarkę XXI wieku [1].

## Początki hakerstwa

Na początku istnieli tak zwani Prawdziwi Programiści. Nie nazywali siebie "hakerami", w ogóle nie nazywali siebie. Wyrażenie "Prawdziwy Programista" powstało dopiero po 1980 roku, zostało stworzone przez jednego z tych zdolnych ludzi. Od 1945 roku technologie komputerowe przyciągały największe i najbardziej kreatywne



komunikacji. Motorem coraz szybszych zmian jest postęp w rozwoju urządzeń IP (Internet Protocol) i sieci optycznych oraz technologii zapewniających bezpieczeństwo i jakość usług. Coraz doskonalsze sieciowe systemy operacyjne, przeglądarki, portale, wyszukiwarki, systemy pracy grupowej, rozproszone bazy danych, protokoły usług katalogowych i wymiany danych sprzyjają tworzeniu i wdrażaniu szerokiej gamy aplikacji. Występuje szeroko rozumiany proces budowy społeczeństwa informacyjnego. Proces przechodzenia do społeczeństwa informacyjnego będzie wymagał zasadniczych zmian w szeroko pojętej infrastrukturze (administracja państwowa i samorządowa, jednostki gospodarcze, każdego szczebla szkoły, ośrodki akademicko – naukowe i badawczo – rozwojowe itp.), kulturze biznesowej, otoczeniu prawnym i organizacyjnym. Dynamiczny rozwój technologii informatycznych w ostatnich kilkunastu latach, w tym Internetu, będzie miał

umysł świata. Od czasów ENIAC-a Eckerta i Mauchly'iego istnieje ciągle nieśmiała grupa entuzjastów programowania, ludzi, którzy tworzą i obsługują programy dla zabawy. Prawdziwi Programiści wywodzili się zazwyczaj z kręgów inżynierów, fizyków. Część z nich związana była z radiem amatorskim. Nosili koszule z poliestru, krawaty i okulary z grubymi szklami, programowali w assemblerze, FORTRANIE i w kilku innych „starożytnych” językach, o których świat zapomniał. Kultura „Prawdziwych Programistów” była mocno związana z przetwarzaniem wsadowym (najczęściej w celach naukowych), które zostało wyparte przez pracę interaktywną, uniwersytety, sieci. Jednak dało to narodziny tradycji, która z czasem zmieniła się w projekt otwartych źródeł hakerskiej kultury [2].

## Pierwsze szkodliwe programy Malware

Malware to ogólnie wszelkiego rodzaju oprogramowanie, które zostało

stworzone w celu wyrządzenia szkód w dowolny sposób osobom, na których komputerach oprogramowanie to funkcjonuje. Programy takie są rozsyłane za pośrednictwem poczty elektronicznej, popularnych komunikatorów, umieszczane do pobrania w postaci linków na różnych stronach WWW. Bardzo często użytkownicy nie są świadomi posiadania na swoich komputerach takiego oprogramowania, dlatego zaleca się korzystanie (i bieżącą aktualizację) z oprogramowania antywirusowego. W skład malware, oprócz wirusów, wchodzi również:

1. Robaki
2. Konie trojańskie
3. Bomby logiczne
4. Króliki, bakterie
5. Spyware
6. Keylogery
7. Dialery

**Robaki** to bardzo podobne do wirusów samodzielnie powielające się programy, rozprzestrzeniające się jednak nie przy pomocy „żywiciela” jak to robią wirusy, lecz za pośrednictwem środków elektronicznego przekazu w Internecie. Głównie za pomocą poczty elektronicznej i komunikatorów internetowych. Robaki powielają się i kopiują na nowe komputery w sposób automatyczny, przejmując funkcje odpowiedzialne za np. komunikację i przesyłanie plików. Rozprzestrzenianie się robaków przyczynia się do zwiększenia ruchu w Internecie i niekiedy „zapychania” całych sieci firmowych.

**Konie trojańskie**, zwane popularnie trojanami, to bardzo sprytne aplikacje, które pod pozorem ciekawych funkcji przemycają na komputer użytkownika niezwykle groźną zawartość. Jak najbardziej na miejscu jest tu nawiązanie do mitologicznego konia trojańskiego, który podstępem, pod pozorem prezentu wprowadził do Troi greckich żołnierzy, którzy następnie zdobyli miasto. Taka jest właśnie rola komputerowych trojanów: podszycują się pod rozmaite aplikacje, a w rzeczywistości dokonują spustoszenia w systemie użytkownika.

**Bomby logiczne** to zagrożenie często przemycane wraz z trojanami.

cd. na stronie 8

Jest to dosyć specyficzne oprogramowanie, aktywujące się dopiero w pewnych określonych sytuacjach, do tego czasu pozostając w stanie nieaktywnym, przez co zagrożenie to jest bardzo trudne do wykrycia.

**Króliki i bakterie** – bardzo sympatycznie nazwane, dosyć prymitywne aplikacje, których właściwie jedynym celem jest zawieszenie zaatakowanego systemu przez masowe powielanie się i zajęcie wszystkich dostępnych zasobów pamięci i czasu pracy procesora. Poza tym aplikacje te nie wykazują niszczycielskich skłonności.

**Spyware** to oprogramowanie szpiegujące działanie użytkownika, gromadzące rozmaite dane i przekazujące je bez wiedzy szpiegowanego do autora programu. Najczęściej programy spyware wykradają prywatne informacje takie jak loginy i hasła do serwisów internetowych, skrzynki email, kont bankowych, numery kart kredytowych, adresy email znajomych, z którymi użytkownik prowadzi korespondencję.

**Keylogger** to program przechwytyjący i zapisujący do pliku wszystkie wpisywane przez użytkownika na klawiaturze znaki, łącznie z nazwami aplikacji, w których użytkownik je wprowadził.

**Dialery** to programy wykonywalne, najczęściej w postaci niewielkich plików EXE, wykorzystujące modem i linię telefoniczną do zestawiania połączenia. Pierwotnie dialery nie były aplikacjami złośliwymi – miały ułatwiać użytkownikom łączenie się z Internetem (dostęp DialUp) czy też z sieciami firmowymi [3].

### Ataki komputerowe

DoS – to atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów. Atak polega zwykle na przeciążeniu aplikacji udostępniającej określone dane czy obsługującej klientów (np. wyczerpanie limitu wolnych gniazd dla serwerów FTP czy WWW), za-

pełnieniu całego systemu plików tak, by umieszczanie dalszych informacji nie było możliwe (w szczególności serwery FTP), czy po prostu wykorzystaniu błędu powodującego załamanie się pracy aplikacji [4].

**Spam** – niechciane wiadomości elektroniczne. Najbardziej rozpowszechniony jest spam za pośrednictwem poczty e-mail. Część użytkowników doświadcza także spamu w komunikatorach (np. Gadu-Gadu). Zwykle (choć nie zawsze) jest wysyłany masowo.

Aby określić wiadomość mianem spamu, musi ona spełnić trzy następujące warunki jednocześnie:

1. Treść wiadomości jest niezależna od tożsamości odbiorcy.
2. Odbiorca nie wyraził uprzedniej zgody na otrzymanie tej wiadomości.
3. Treść wiadomości daje podstawę do przypuszczeń, że nadawca wskutek jej wysłania może odnieść zyski nieproporcjonalne w stosunku do korzyści odbiorcy [5].

**Phishing** – wyludzanie poufnych informacji (np. haseł lub szczegółów karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne. Jest to rodzaj ataku opartego na socjotechnice. Dzisiaj przestępcy sieciowi wykorzystują techniki phishingu w celach zarobkowych. Popularnym celem są banki czy aukcje internetowe. Phisher wysyła zazwyczaj spam do wielkiej liczby potencjalnych ofiar, kierując je na stronę WWW, która udaje rzeczywisty bank internetowy, a w rzeczywistości przechwytyje informacje wpisywane tam przez ofiary ataku [6].

### Rady bezpieczeństwa dla użytkowników Internetu

Wystarczy chwila nieuwagi, dosłownie jedno nieuważne kliknięcie odnośnika, pliku załącznika czy przycisku „OK” w okienku instalatora i już użytkownik „ma problem” w postaci nieproszonego gościa. A jego pozbycie się wcale nie jest takie proste.

Po pierwsze: należy unikać miejsc, w których możemy zostać narażeni na „atak” wszelkiej maści darmowych i pochodzących z niepewnego źródła wygaszaczy ekranu, zestawów ikon i tapet, gier, czy dodatków rzekomo mających usprawnić korzystanie z komputera, a w rzeczywistości niosących groźną zawartość w postaci spyware, dialera czy bomby logicznej. Programy i dodatki do systemu operacyjnego należy pobierać wyłącznie z zaufanych serwisów, w których ryzyko pojawienia się programu o szkodliwym działaniu jest minimalne. Po drugie: należy bezwzględnie mieć zainstalowany i regularnie uaktualniany program antywirusowy. Jeśli użytkownik jednak nie posiada takiego oprogramowania, powinien często sprawdzać stan bezpieczeństwa dostępnymi skanerami online [3]. Po trzecie: należy używać Windows Update w celu skanowania i aktualizacji systemu operacyjnego Windows za pomocą najnowszych, darmowych poprawek oprogramowania, łącznie z przeznaczonymi dla programów Microsoft Internet Explorer i Microsoft Outlook Express. Po czwarte: należy zainstalować zaporę sieciową w celu zablokowania szkodliwego oprogramowania lub intruzów atakujących przez Internet lub sieć lokalną. Po piąte: nie należy otwierać załączników e-mail od nieznannej osoby. Konieczne jest również zachowanie ostrożności w przypadku osób znanych. Należy uważać na nieznaną witryny WWW, ponieważ mogą one przenieść wirusa na komputer [7]. Przestrzegając powyższych zasad bezpieczeństwa użytkownik minimalizuje swoją ekspozycję na zagrożenia jakie niesie ze sobą poruszanie się w Internecie. Podsumowując – ogólne zasady opierają się na zdrowym rozsądku i zabezpieczeniu programowym. Cała masa ciągle rozwijanych programów antywirusowych gwarantuje szeroki wybór rozwiązań zabezpieczających.

### Bibliografia

- [1] <http://www.umk.pl/~zenkiewicz/kalendarium/>
- [2] [http://pl.wikisource.org/wiki/Krótką\\_Historia\\_Hakerstwa](http://pl.wikisource.org/wiki/Krótką_Historia_Hakerstwa)
- [3] [http://bezpieczenstwo.onet.pl/1416377,item,0,Konie\\_robaki\\_kroliki\\_i\\_bakterie\\_czyli\\_malware\\_jest\\_grozny,artykuly.html](http://bezpieczenstwo.onet.pl/1416377,item,0,Konie_robaki_kroliki_i_bakterie_czyli_malware_jest_grozny,artykuly.html)
- [4] <http://pl.wikipedia.org/wiki/DoS>
- [5] <http://pl.wikipedia.org/wiki/Spam>
- [6] <http://pl.wikipedia.org/wiki/Phishing>
- [7] [http://www.alarmowesystemy.info/index.php?option=com\\_content&task=view&id=16&Itemid=97](http://www.alarmowesystemy.info/index.php?option=com_content&task=view&id=16&Itemid=97)