Coraz szybciej, coraz lepiej – historia komputerów zdaje się pasmem samych sukcesów. Jednak pozory mylą. Producenci lubią zapowiadać swoje wyroby, jako przełomowe innowacje na rynku komputerów. Ale gdy któreś urządzenie okaże się niewypałem, wszyscy nabierają wody w usta. Na liście największych wpadek

sprzętowych można pokazać wiele urządzeń znanych firm. Sprzęt komputerowy rozwija się w zabójczym tempie. Wystarczy jeden błąd, aby doprowadzić renomowaną firmę do bankructwa. Ta branża jest bezwzględna. Atari, Commodore, Nixdorf, Olivetti, Zenith to tylko kilka przebrzmiałych marek minionych czasów.

Od kiedy istnieje oprogramowanie, producenci usiłują chronić je przed niedozwolonym kopiowaniem. Jednak żadne zabezpieczenie nie stanęło na wysokości zadania. Przemysł fonograficzny lamentuje z powodu pirackiego kopiowania albumów, a producenci filmów i oprogramowania skarżą się na

miliardowe straty przez nielegalne duplikowanie nośników. Temat zabezpieczania przed kopiowaniem nie schodzi z nagłówków branżowych pism i gazet. Trudno uwierzyć, że walka między firmami próbującymi bronić sprzedawanych treści i podziemną sceną crackerów ma aż tak długą tradycję. Już w połowie lat

osiemdziesiątych, czyli za czasów sprzętu typu: Commodore 64, uprawia się na dużą skalę wymianę złamanego oprogramowania – przede wszystkim gier. Tymczasem producenci dwoją się i troją, aby uniemożliwić kopiowanie dyskietek. Niektóre mechanizmy działają na zasadzie zaszyfrowanych lub ukrytych plików

umieszczonych na oryginalnych nośnikach. Zwyczajna kopia na nic się nie zda, bo uruchamiany program sprawdza, czy na dyskietce znajdują się odpowiednie pliki. Powstają też specjalne programy, które bit po bicie kopiują zawartość oryginału wraz z zabezpieczeniem. O uśmiech wzruszenia

przyprawiają próby ochrony oprogramowania za pomocą mechanicznego zabezpieczenia dyskietek przed omyłkowym zapisem. Aby uruchomić skopiowany program, wystarczy zalepić kawałkiem taśmy samoprzylepnej wyżłobienie znajdujące się na krawędzi dyskietki. Producenci gier stosują jeszcze inne

metody. Przed uruchomieniem gry trzeba wpisać określone słowo z instrukcji obsługi albo kod ustalony przy użyciu dołączonej tarczy obrotowej. Drogie aplikacje CAD są zabezpieczone sprzętowo. Przed uruchomieniem programu trzeba umieścić specjalną zaślepkę w porcie równoległym. Sprytni programiści

potrafią obejść i taki mechanizm. Wraz z wprowadzeniem na rynek płyt CD i DVD producenci próbują nowych sposobów zabezpieczania przed kopiowaniem. Jednak nawet one nie zdają egzaminu. Takie metody jak np. kod regionalny można obejść przez modyfikację wewnętrznego oprogramowania urządzenia

odtwarzającego. Po pewnym czasie w Internecie wręcz roi się od witryn udostępniających narzędzia do łamania zabezpieczonych gier. Począwszy od 2000 r. przemysł fonograficzny wyposaża płyty Audio CD w zabezpieczenia przed kopiowaniem. Mimo pasma porażek producenci nie dają za wygraną, ciągle udoskonalając

metody zabezpieczania nośników. Przyszłość wykaże, czy uda im się dopiąć swego. Wydaje się jednak, że mają marne szanse. Innym zagrożeniem stały się wirusy. Cyfrowa plaga wzięła swój początek niespełna 30 lat temu z niepozornej gry. Późniejszy założyciel firmy Autodesk produkującej oprogramowanie CAD,

dostaje liczne prośby od kolegów z pracy o udostępnienie jego gry komputerowej o nazwie „Animals”. Pozytywnie rozpatrując prośby swoich kolegów umieszcza w gry procedurę automatycznego kopiowania. W momencie uruchomienia gra samodzielnie duplikuje się do wszystkich katalogów, do których ma dostęp dany

użytkownik. W takich właśnie okolicznościach narodził się pierwszy wirus. Co prawda nieszkodliwy, ale bardzo irytujący. W mgnieniu oka Animals rozprzestrzenia się w całej sieci firmowej. W ten sposób narodziła się potrzeba napisania pierwszego programu antywirusowego, który zastąpił szkodnika

niegroźną wersją gry. Od tego czasu zaczynają się pojawiać wirusy, które np. atakują komputery osobiste. Robak Morris, zawdzięczający swą nazwę autorowi, nie miał zamiaru wyrządzić nikomu krzywdy, jednak błąd w kodzie programu sprawił, że wirus sparaliżował niejeden serwer. Idealne warunki

rozmnażania się znajdują wirusy i robaki w środowisku Windows. Umożliwia to brak mechanizmów do zarządzania uprawnieniami w tak poważnych narzędziach, jak Host skryptów. I tak oto, dobrodziejstwo w postaci posiadania komputera, przeradza się w paraliżujący stres, czy aby ten komputer będzie działał bez

zarzutów, czy aby nie zaatakują go wirusy lub robaki. W zależności od ich rodzajów utracimy tylko trochę (jakieś pliki) albo będziemy musieli kupić sobie całkiem nowy sprzęt bo poprzedni „robaki i wirusy zjadły”.