Prečítali sme za Vás.

V čísle ISACA žurnálu (http://www.isaca.org/Journal/Current-Issue/Pages/default.aspx) nás zaujal článok o kyberkriminalite – Porozumieť vlne kyberkriminality (http://www.isaca.org/Journal/Past-Issues/2014/Volume-1/Pages/Understanding-the-Cybercrime-Wave.aspx).

Autor Tommie Singelton, pripravil Miroslav Molnár

(http://www.isaca.org/profile/pages/default.aspx?accountname=ISGFormProvider:048624) sa v článku pútavým spôsobom venuje súčasným trendom vo svetovej kyberkriminalite. Ako sám autor v článku uvádza, v súčasnej ére rozšírenia informačných technológií nie je otázkou ČI ale KEDY sa sami stanete objektom hackerov či iných kyberkriminálnikov.

Najčastejším objektom útočníkov v kyberpriestore sú finančné inštitúcie, kde hlavným cieľom je okamžité obohatenie sa prostredníctvom prevodu prostriedkov na účet útočníka, či ukradnutie identity klienta (PII – „Personable Identifiable Information“) a pomocou nej vydanie kreditnej karty či úveru na neoprávnenú osobu – útočníka. Ďalším cieľom útočníkov bývajú spoločnosti, v ktorých sa za tovar či služby platí cez web pomocou kariet (http://tech.sme.sk/c/7064817/hackeri-naburali-v-usa-obchody-ziskali-miliony-udajov.html). Ukradnutie informácií o kartách umožňuje ich zneužitie na neoprávnené nákupy tovaru alebo služieb v prospech útočníka.

Hoci priamy finančný prospech je najčastejším dôvodom kyberútokov, existuje aj nemalá skupina hackerov a kyberútočníkov, ktorých cieľom sú rôzne vládne organizácie a citlivé dáta štátnych či veľkých súkromných firiem. Tieto skupiny kyberútokov sú podporované a riadené na štátnej úrovni a v praxi tak denne dochádza ku kybervojnám medzi jednotlivými štátmi (spomeňme tu známu aféru ohľadne vírusu Stuxnet – viď napr. http://tech.sme.sk/c/5469934/novy-virus-moze-byt-urceny-na-priemyselnu-spionaz.html).

Nové technológie, napr. v oblasti kryptografie, doniesli aj nové metódy útokov. Pri neopatrnej manipulácii s prílohami z nevyžiadaných e-mailov môže dôjsť k nakazeniu počítača a v priebehu pár dní po napadnutí k úplnému zašifrovaniu a znefunkčneniu počítača a všetkých dát na ňom. Útočník následne ponúka odkúpenie šifrovacieho kľúča za odmenu 300 – 500 dolárov (http://tech.sme.sk/c/7009753/britania-hlasi-masivne-rozoslanie-sifrovacieho-virusu.html). Pokiaľ napadnutý nemá zálohované dáta, tak na získanie vlastných dát mu neostáva nič iné, len útočníkovi zaplatiť.

Okrem technických prostriedkov, používajú kyberútočníci aj sofistikovanejšie metódy sociálneho inžinierstva ako v prípade ukradnutia účtu na sociálnej sieti Twitter (podrobnosti viď článok http://tech.sme.sk/c/7086388/ako-prisiel-programator-o-50-tisic-dolarov.html).

Podľa autora článku sa kyberútočníci zameriavajú buď na malé a stredné podniky, kde je predpoklad nižších nákladov na IT bezpečnosť a tým menšia miera bezpečnostných opatrení a zároveň vyššia pravdepodobnosť získania údajov o kreditných a debetných kartách a transakciách, alebo na inštitúcie s veľkým objemom finančných dát, kde v záujme získania bohatej „kyberkoristi“ je ochotný útočník investovať viac času aj prostriedkov s vidinou ich rýchlej návratnosti.

Ako sa týmto trendom najlepšie brániť? To už sa dozviete priamo v článku. Téme kyberkriminality sa ISACA venuje okrem toho aj na svojich stránkach http://www.isaca.org/Knowledge-Center/Research/Pages/Cybersecurity.aspx.