Našel chyby Starbucksu. Od firmy už dostal tisíce dolarů

Weby jsou zranitelné, jenže velké firmy si zranitelnost nemůžou dovolit. Proto některé vyhlašují speciální výzvy pro IT odborníky, aby jim pomohli slabá místa v zabezpečení systémů najít. K jedné takové se přidal i student fakulty informatiky Patrik Hudák.

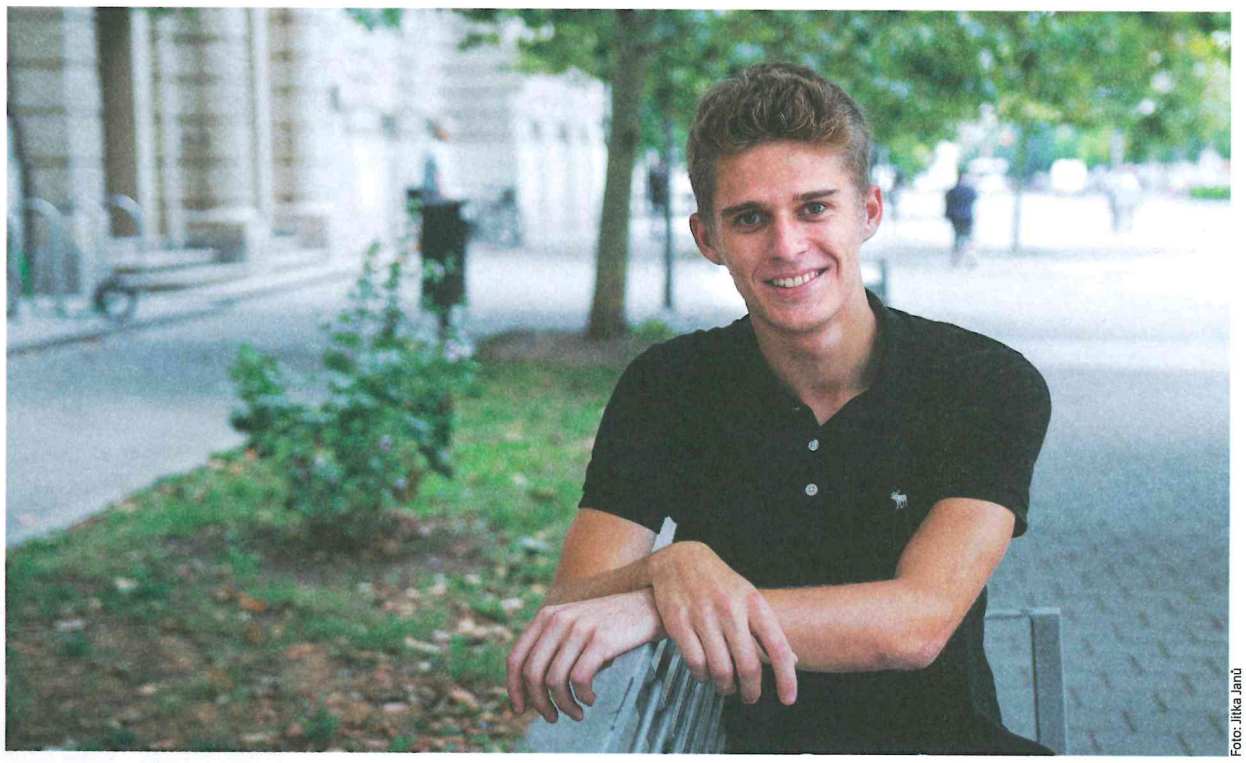

Foto: Jitka Janů

Kávovému řetězci Starbucks pomohl odhalit problém, který nakonec firma ocenila dvěma tisíci dolarů. A pak ještě jeden odměněný stejnou sumou. Zabezpečení webů je Hudákovo velké téma. Psal o něm už bakalářku a teď na jaře i magisterskou práci, kterou úspěšně obhájil na výbornou.

Už při škole navíc pracoval pro jeden bezpečnostní start-up, který se podílí na vylepšení zabezpečení webů firem. Lidé jako on dokážou velmi dobře vyhmátnout i nové typy zranitelností a přesně do této kategorie spadal i problém, který Hudák našel u webu kávového řetězce jako první.

Zatím si ho uvědomuje jen málo odborníků, natož firem, takže řešit se ho daří jen pomalu a postupně. Konkrétně tuto zranitelnost popisuje jen několik málo odborných textů, a to přesto, že případy, kdy se něco takového objevilo, jsou staré už nejméně čtyři roky. Shrnout se to dá pod pojem převzetí subdomény a hodně to souvisí s využíváním cloudových služeb, tedy virtuálních úložišť.

„Pokud chcete například vytvořit e-shop, můžete si ho udělat na svém serveru, nebo využít cloudovou službu, což má za určitých podmínek svoje výhody. Koncový uživatel to nepozná, protože e-shop má adresu, která se tváří jako vaše, ta reálná je ale jiná, odkazuje totiž i na poskytovatele služby," naznačuje Hudák.

Aby došlo k propojení poskytovatele cloudu a webu objednavatele služby, musí se vytvořit elektronické spojení obou stran. A právě to může být později problematické. Když objednavatel službu přestane potřebovat a přestane ji platit, „jeho" webová adresa už bude nefunkční, ale napojení na jeho web zůstane živé. Když si pak někdo jiný objedná službu a záměrně si řekne o stejnou adresu, dokáže se pak virtuálně tvářit jako původní majitel a využít toho k nekalému jednání.

Hudákova práce upozorňuje na problematičnost využívání cloudových služeb, které jsou ale čím dál oblíbenější.

Tento základní popis může nabírat při reálném použití různá specifika. Hudák ho popsal ve své diplomce a k tomu si vytvořil nástroj na ověřování domén, aby našel konkrétní příklady a svoji teorii potvrdil i v reálném technickém životě. Zaměřil se přitom na firmy, které pomoc tohoto typu honorují nebo oceňují aspoň nějakou jinou formou, aby si na tom ještě jako student udělal jméno.

„V případě Starbucksu spočívala první zranitelnost v doručování obsahu webu, který je pro zajištění větší rychlosti umístěný na různých serverech na různých místech. Díky tomu jsem byl ale schopný kontrolovat obsah domény," popisuje Hudák, který našel něco jako boční zapomenutý vchod. S jeho využitím mohl na web umisťovat jakýkoliv vlastní obsah.

Najít takový boční vchod není jednoduché, a pokud se to povede, není takových možností moc. Proto když Hudák chybu, kterou našel, firmě hlásil, označil ji jako málo nebezpečnou. „Proto mě to dost překvapilo, když sama společnost klasifikaci za dva dny změnila na vysokou. Nabízel jsem jim i pomoc, ale nikdo se neozval. Čtyři měsíce se nic nedělo a potom mi v červenci přišel e-mail, že děkují, případ uzavřeli a posílají mi dva tisíce dolarů," vypráví Hudák.

Částka ho překvapila. Běžné jsou odměny v řádu stovek dolarů. Další překvapení nastalo, když našel čerstvý absolvent u stejné firmy obdobnou chybu a ona mu vyplatila další dva tisíce dolarů. Hudák má hlavně na honorované programy čich. Na internetu má i vlastní stránku, kde se může každý podívat, komu všemu a jaké problémy reportoval.

Aktuálně zvažuje také to, že by si založil vlastní bezpečnostní start-up. Podobná odhalení podle něj budou přibývat. Poskytovatelé cloudových služeb totiž zatím před problémem spíš zavírají oči. Zájemci většinou pronajmou cloudový prostor pod názvem, o jaký si řekne, aniž by cloudový poskytovatel ověřoval, jestli se tím nezasahuje do vlastnických práv někoho jiného.

Martina Fojtů

Studenti jezdí nově za čtvrtinu ceny

Všichni studenti do 26 let mohou od začátku září jezdit vlaky a autobusy po celé České republice za čtvrtinu ceny. Začalo totiž platit nařízení vlády, které dopravcům 75procentní slevu proplácí ze státního rozpočtu. K jejímu získání je potřeba pouze platný průkaz ISIC (musíte mít přelepku) nebo žákovský průkaz.

Sleva se týká všech studentů, kteří budou schopni u průvodčího jednou z těchto cest prokázat svůj studentský status nehledě na státní příslušnost. Obavy tak nemusejí mít třeba Slováci dojíždějící za studiem do Brna. Výrazně zlevněnou jízdenku je nyní možné zakoupit do všech spojů Českých drah ve 2. vozové třídě, do všech vlaků i autobusů společnosti Regiojet ve třídách Low Cost, Standard a Relax i u dalších dopravců. Nezáleží už přitom, jestli student cestuje do školy nebo třeba na výlet.

Jediné omezení platnosti slev představuje státní hranice. Při cestách do zahraničí budou studenti za zbývající část trasy platit plnou cenu. Nově také není možné studentskou slevu kombinovat s jakoukoliv další slevou. Týká se to především oblíbených In karet, které většina studentů doposud využívala. Jakoukoliv platnou aplikaci na In kartě je nyní možné vrátit a České dráhy vyplatí poměrnou část její ceny podle doby, která zbývá do konce její platnosti.

„Studenti ale nemusí spěchat, vrácení je možné provést kdykoliv až do konce dubna 2019 a proplacená částka se bude vždy počítat od 1. září," vysvětlil Roman Šulc z Českých drah.

Slevy se týkají kromě vlaků jen dálkových a příměstských autobusů, městské hromadné dopravy tedy nikoliv. Přesto však některá města či kraje chystají vlastní slevy, kterými chtějí zabránit zmatkům při přestupech v rámci integrovaných systémů či chtějí sjednotit podmínky v dopravě obecně.

Kompletní seznam měst či krajů, kde dojde ke zlevnění jízdného i v MHD, ještě není znám, slevu ve stejné výši ale už oznámily třeba Liberecký a Ústecký kraj a k menším změnám dojde i v Brně. Vznikne zde nový typ předplatní online jízdenky, jejíž cena se bude postupně snižovat, bude-li přímo navazovat na předešlou jízdenku.

K získání slevy je nově potřeba jen platný ISIC.

Martin Vérteši

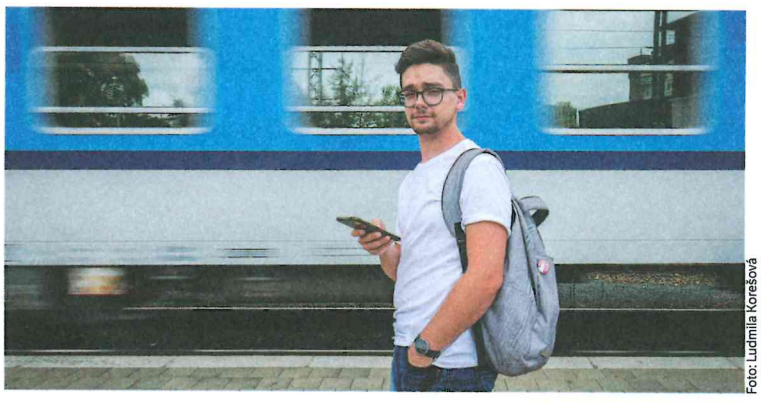

Foto: Ludmila Korešová