TISKOVÁ ZPRÁVA

Pokémon GO!: Ztraťte je všechny, aneb Pokémoni na pracovišti?

Pro firmy se tato hra stává noční můrou bezpečnosti

Praha, 23.8 - Pokémon GO! se stalo fenoménem, na kterém „ujíždí“ lidé všech věkových kategorií. Miliony hráčů po celém světě chytají oblíbené příšerky, které po bezmála 20 letech znovu katapultovaly tržní hodnotu Nintenda o téměř třetinu. Podobně jako u jiných masivně rozšířených platforem, již od začátku Pokémon GO! otevírá diskuze ochrany soukromí a bezpečnosti informací.

Na obecné úrovni jde o stejné problémy, o kterých se mluví již dlouho – informace o poloze, chování uživatele a uživatelském účtu jsou všechno citlivá data, která mohou být zneužita různými způsoby. A bohužel, lákadlo hry je natolik veliké, že způsobuje tendenci zapomínat na důsledky a akceptovat synchronizaci veškerých údajů, o které si aplikace řekne. Krádeže identity a cílené zločiny se mohou sice zdát vzdálenou hrozbou amerických filmů, Pokémon GO! však uvedl novou generaci možností zneužití.

Ve hře mají například hráči možnost použít předmět *Lure*, který po určitou dobu láká Pokémony na určené místo a je viditelný i pro ostatní uživatele. Tato místa (a také například stadiony, kde mohou hráči s Pokémony bojovat) se stávají vyhledávanou lokací nadšených trenérů, kteří do své mobilní sbírky shánějí další přírůstky. Také však mohou dostat nepozorné hráče na odlehlá místa, kde se stávají snadnou kořistí zlodějů. Již několik týdnů od vydání hry byla hlášena ozbrojená přepadení a krádeže právě v místech, kde lidé pohroužení do hry nepozorovali blížící se nebezpečí a velice rychle na to doplatili.

Pohlcení virtuální realitou může způsobit nepříjemné následky každému nepozornému hráči. Do budoucnosti můžeme očekávat pravděpodobně ještě více podobných situací. Výměny příšerek nebo boj mezi hráči, o kterých se diskutuje zatím jenom mimo oficiální vyjádření Nianticu, mohou přinést další zajímavé problémy ochrany soukromí, pokud budou pracovat s aktuální lokalitou trenéra.

Když se zamyslíme nad dopadem používání Pokémon GO! ve firemním prostředí, problémy se ještě znásobí. Pro organizace, operující na projektech podléhajících utajení, jde o noční můru bezpečnosti. Například Izraelská armáda nedávno zakázala jednotkám aplikaci využívat, a to zejména z důvodu rizika odhalení tajných základen. Jeden z argumentů proč hru zakázat byl i fakt, že pro útočníky není složité podvrhnout aplikaci, která bude vypadat stejně, ale informace o poloze bude zasílat nepřátelským jednotkám. Hra také kromě polohy využívá fotoaparát, což byl jeden z důvodů, proč dostala striktní NE na pracovištích

automobilek, jako jsou Volkswagen nebo Škoda Auto. Pokémony si nezachytáte například ani v Pentagonu.

Když vezmeme do úvahy běžné firemní zařízení, s velkou pravděpodobností bude obsahovat také firemní data. Minimem jsou v dnešní době kontakty, většina zaměstnanců si také synchronizuje firemní poštu, která obsahuje téměř celou pracovní agendu uživatele. Pokud dá organizace lidem neomezenou možnost instalace aplikací, vystavuje se tím riziku. Nejde totiž ani v tomto případě jenom o samotnou aplikaci Pokémon GO! – šikovnější uživatele používají rozšíření nebo boty, které jim ulehčují práci, přičemž se jedná často o neověřené a neznámé programy. A nejde také pouze o zaměstnance samotné – kdo by nedovolil občas dětem zahrát se na mobilu oblíbenou hru?

„Pokud nad hraním Pokémon GO! jenom přemýšlíte, doporučujeme zamyslet se nad tím, jaké všechny informace budete vy (nebo vaši zaměstnanci) sdílet s výrobcem a do budoucna také možno s veškerým okolím“ říká Petr Žikeš, CEO společnosti Safetica Technologies a dodává: *„Osobní data mohou být velice snadno zneužity útočníkem, který má širokou škálu možností jak vás napadnout prostřednictvím zařízení i komunikace na síti. Pro ty, kteří se navzdory tomu rozhodnou aplikaci používat, doplňujeme alespoň několik tipů, jak zajistit co nejbezpečnější chytání digitálních příšerek:“*

- Nezapomínejte při hraní na své okolí. Buďte obezřetní zejména na společných místech, viditelných pro všechny trenéry.
- Nehrajte během řízení, aneb #dontpokemongoanddrive
- Nezapomínejte na bezpečnost svého zařízení. Používejte antivirus, neinstalujte aplikace z nedůvěryhodných zdrojů, nezapínejte vývojářský mód, pokud ho nepotřebujete. Všechny důležité aplikace včetně systému udržujte v aktuálních verzích.
- Vyhněte se veřejným Wi-Fi sítím. Pokud je vyloženě nutné je použít, vyhledávejte technologii WPA2, chráněné heslem.
- Pro firemní prostředí je možné použít MDM (Mobile Device Management) řešení, které umožní řídit bezpečné nastavení na firemních zařízeních a také provádět audit nebo omezování nainstalovaných aplikací.

O společnosti Safetica Technologies
Safetica Technologies se specializuje na softwarovou ochranu proti úniku citlivých dat a a ztrátami spojenými s neefektivně vynaloženými IT a personálními náklady. Safetica je technologickým partnerem globální antivirové společnosti Eset a mezi distribučními partnery jsou také zkušení systémoví integrátoři. Produkty společnosti a jejich podpora jsou dostupné ve více než 50 zemích světa a aktuálně zabezpečuje přes 28000 zařízení.

Pro více informací navštivte internetovou stránku: www.safetica.cz

TISKOVÁ ZPRÁVA

Pro více informací prosím kontaktujte:
Martin Moc, Weber Shandwick, e-mail: mmoc@webershandwick.cz, tel. 724 724 280