Benjamin Král (Avast)

Kybernetická bezpečnost očima etického hackera

MICHALA BENEŠOVSKÁ

Benjamin Král je etický hacker neboli penetrační tester ve společnosti Avast. Co vlastně obnáší práce etického hackera? Jak jsou na tom české firmy s bezpečností? Které hrozby jsou aktuálně na vzestupu? A jak lze rozvíjet a podporovat mladé talenty v oblasti kybernetické bezpečnosti? To vše nám Ben objasnil.

Můžete uvést, jak jste se dostal k práci etického hackera?
Po vystudování Vysokého učení technického v Brně jsem se přidal k bezpečnostnímu týmu Masarykovy univerzity CSIRT-MU, kde jsem z pozice forenzního specialisty řešil bezpečnostní incidenty a pomáhal chránit síť Masarykovy univerzity, respektive její uživatele, před kybernetickými hrozbami. V polovině minulého roku jsem pak přešel z defenzivy na ofenzivu, a v současné době pracuji jako etický hacker, respektive penetrační tester ve společnosti Avast.

Jak vypadá váš běžný pracovní den – co je náplní práce etického hackera? Kdo jsou vaši „klienti“?
Mojí pracovní náplní je útočit na počítačové systémy a obecně řečeno testovat zabezpečení aktiv společnosti Avast. Mým „klientem“ je tedy v zásadě vždy Avast. To ale samozřejmě neznamená, že hackuji pouze systémy vyvinuté společností Avast. Neboť Avast jako většina (obdobných) firem používá různé externí produkty a služby, které často pracují s citlivými firemními daty, a tudíž chyba v těchto produktech by mohla být taktéž bezpečnostní hrozbou vedoucí ke ztrátě, pozměnění či prozrazení takových dat. Mým cílem je tedy nalézt zranitelnosti a nedostatky v různých produktech, systémech a procesech, aby mohly být odstraněny dříve, než je zneužije případný útočník. A to jak v produktech společnosti Avast, tak i v produktech předních světových technologických firem, jež Avast používá.

Co vás na práci etického hackera nejvíc baví?
Jednoznačně nejlépe hodnotím rozmanitost práce. Jeden penetrační test typicky trvá dva až tři týdny a každý je unikátní. Někdy se pokouším obejít detekci antiviru naprogramováním sofistikovaného malwaru, jindy hackuji důležitý informační systém, napadám mobilní aplikaci nebo se snažím napadnout firemní Wi-Fi síť. Při této práci se člověk opravdu nenudí, každý den přináší novou výzvu k pokoření. A pocit, kdy nakonec uspěji a najdu zranitelnost, která by při zneužití útočníkem měla vážný dopad na stovky tisíc uživatelů po celém světě, je tou nejsladší odměnou, jež se mi, věřím, nikdy neomrzí.

Jak jsou na tom podle vás české firmy s kybernetickou bezpečností? Co je jejich největší problém?
Kybernetická bezpečnost je pro každou firmu výdajem, který se snaží držet na takové úrovni, na jakou odhaduje riziko vycházející z kybernetických hrozeb. Některé firmy dokážou tohle riziko správně odhadnout, sehnat schopné lidi a ochranu svých aktiv dostatečně financovat. Jiným firmám se toto buď nedaří, nebo kybernetickou bezpečnost neřeší vůbec, a pak je jen otázkou času, než na to doplatí. Jako problém v oblasti kyberbezpečnosti tedy vidím podfinancování. Když firma nevyvine dostatečnou snahu se správně chránit, jednou na to doplatí. A taková snaha stojí lidské úsilí a peníze.

Jak se dá dnes spolehlivě chránit? Na co by neměly společnosti zapomínat ve své kyberbezpečnostní strategii?
Hlavní motivací útočníků je většinou vydělat peníze ideálně s co nejmenším vynaloženým úsilím. Typickým cílem je, dle očekávání, nejslabší článek, což je v našem případě člověk. Nalezení a následné zneužití kritické zranitelnosti ve složité počítačové síti je komplikovaný a časově náročný proces vyžadující mnoho vědomostí a zkušeností. Oproti tomu odeslat šikovně sepsaný spear-phishingový e-mail několika zaměstnancům dokáže i méně sofistikovaný útočník za pár desítek minut. Jediné, co stojí v cestě ke katastrofě, je bystrý, vzdělaný a podezřívavý zaměstnanec. Rozhodně by tedy měl být nedílnou součástí kyberbezpečnostní strategie program vzdělávání zaměstnanců, který vhodně doplní ostatní technické ochranné prvky společnosti.

Co jsou obecně momentálně největší trendy v oblasti kyberbezpečnostních hrozeb? Velmi oblíbený je mezi útočníky zejména ransomware, proč je tomu tak?
Nejčastější jsou dnes dva typy hrozeb. Prvním jsou útoky na počítačové systémy využívající známé zranitelnosti, spoléhající na to, že zodpovědná osoba zapomněla nebo nestihla systém patřičně aktualizovat. Druhým je útok na již dříve zmíněný nejslabší článek – lidi, nejčastěji právě prostřednictvím phishigových e-mailů. Oba typy útoku však popisují pouze způsob, jakým se útočník do systému dostane. Pak se naskýtá mnoho možností, jak s nově napadeným strojem naložit. Nejčastějším cílem je, dle očekávání, finanční profit. Toho lze dosáhnout různými způsoby – zneužití zařízení k těžbě kryptoměn, monitorování uživatele s cílem získat přihlašovací údaje do banky nebo čísla kreditní karty nebo zmíněným ransomwarem. Ten má však oproti ostatním metodám několik zásadních

výhod – poměrně rychle zašifruje důležitá data a v tu chvíli už je obvykle pozdě s ním cokoliv dělat. Pak už zbývá buď zaplatit výkupné, obnovit data ze zálohy, pokud jsou k dispozici, nebo přijmout ztrátu. A aby toho nebylo málo, tak se ransomware často po úspěšném nakažení nekontrolovaně šíří po síti a dále napadá desítky nebo stovky počítačů současně. Obnova ze záloh může být v takovém případě časově náročná, a firma kolikrát raději zaplatí tučné výkupné, než aby byla dny či někdy až týdny mimo provoz. Takový výpadek totiž vesměs generuje násobně větší ztrátu, než tvoří výše výkupného.

Kam se budou podle vás vyvíjet kybernetické hrozby? Zdá se, že jsou útočníci vždycky o krok napřed... Budou společnosti, které se zabývají bezpečností, schopné adekvátně reagovat a nabídnout odpovídající řešení?
Dle mého názoru bude nadále docházet jak k nárůstu počtu kybernetických hrozeb, tak i k inovacím ve výše zmíněných technikách. Aktuální modus operandi útočníkům funguje, tudíž jde převážně o zvýšení efektivity v jeho provádění. Nově vznikající technologie, jakými jsou například strojové učení a umělá inteligence, se budou velice hodit i útočníkům ke zdokonalování překladů phishingových e-mailů do více jazyků, což povede k větší proliferaci a vyšší úspěšnosti phishingových kampaní.

Rostoucí popularita kryptoměn umožní lépe skrýt pohyby a extrahovat zisky z ilegálních aktivit. Samozřejmě budou vznikat i nové techniky a hrozby, ale predikce jejich konkrétnější podoby se blíží věštění z křišťálové koule. Ruku v ruce s rostoucí intenzitou hrozeb bude stoupat poptávka po odpovídajících bezpečnostních řešeních, což bude hrát do karet právě společnostem zabývajícím se kyberbezpečností. Z toho lze usuzovat, že i v budoucnu bude tento souboj v kyberprostoru vyrovnaný, přibližně tak jako je dnes.

Byl jste trenérem českého národního týmu v ECSC a nedávno jste se stal jedním ze tří trenérů evropského týmu, který se chystá na první mezinárodní soutěž, která právě vzniká. Jak takový „trénink“ vlastně vypadá? Čím jsou podle vás akce typu ECSC přínosné?
European Cyber Security Challenge (ECSC) a nově vznikající International Cyber Security Challenge (ICSC) jsou velmi přínosné akce pro vzdělávání budoucích generací kyberbezpečnostních odborníků.

Každý evropský stát, respektive každý kontinent, sestaví tým těch nejlepších a nejtalentovanějších středoškoláků a vysokoškoláků. Ti se pak sjedou na finále, konající se v jedné z účastnických zemí (letos hostí Česká republika), aby poměřili své síly. Na typickém tréninku řešíme podobné úlohy, jako jsou na finálových soutěžích, případně se účastníme specializovaného workshopu, abychom rozšířili své znalosti, a byli tak lépe připraveni na samotné finále. Rozhodně se ale nejedná o žádnou hru pro děti. Soutěží tohoto typu se účastní i ostřílení veteráni, úlohy často vycházejí z praxe a jsou opravdu značně obtížné. V českém národním týmu je každý rok výběr těch vskutku nejschopnějších mladých talentovaných studentů, kteří jsou často vědomostně na úrovni hackerů z praxe. Členové týmu pak vlastně hravou formou mohou řešit složité kyberbezpečnostní problémy již třeba na střední škole, a tím získat mnohem dříve spoustu zkušeností a znalostí, což jim může poskytnout raketový start do profesního života. Nadto navážou kontakty s ostatními talentovanými studenty, a mají-li zájem, najdou si velmi solidně placenou brigádu u jedné z mnoha zapojených firem, jež trénink či nadcházející finále ECSC 2021 v Praze sponzorují.

Pikantní otázka na závěr: když máte takové schopnosti, nenapadlo vás někdy přejít na „temnou stranu“? Nebylo by to „lukrativnější“?
Lukrativnější by to s největší pravděpodobností bylo, nicméně překročení této hranice s sebou přináší řadu „benefitů“, po kterých rozhodně netoužím. I na „světlé straně“ se touto prací dá slušně uživit, navíc bez obav z případného trestního stíhání a nutností praní špinavých peněz. Není nad to usínat s klidným svědomím z dobře odvedené práce, která nemá destruktivní dopady na život ostatních.