Jak se brání univerzitní sítě

Informační systém, e-mailové adresy zaměstnanců, wi-fi, servery, ohromné množství dat z výzkumů. To všechno se dnes používá nebo vzniká na Masarykově univerzitě a všechno je potřeba chránit proti zneužití. Univerzita na to má sofistikované systémy a spoustu expertů. Seznamte se s tím, jak pracují.

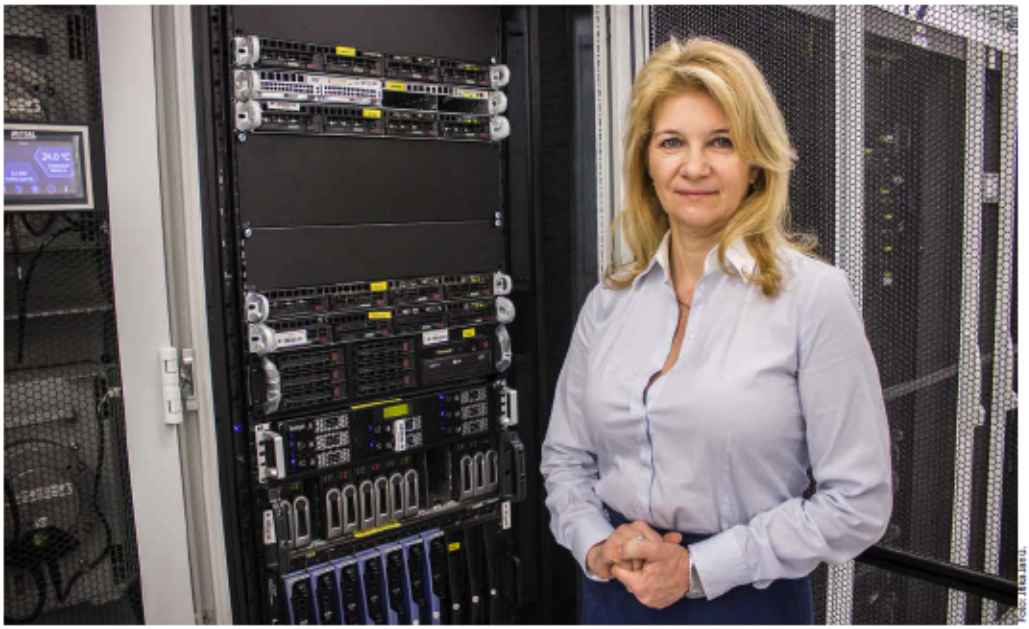

Foto: Jiří Jarů.

Každý student nebo zaměstnanec univerzity denně aktivně využívá řadu nástrojů a většinou nijak zvlášť nepřemýšlí nad tím, díky čemu fungují. Přitom je to komplikovaný a poměrně nákladný úkol.

„Jen za minulý rok bylo odhaleno a aktivně potlačeno asi 82 tisíc pokusů o narušení bezpečnosti infrastruktury univerzity. Jinak řečeno k takovýmto docela standardním útokům docházelo průměrně 225krát denně," naznačuje rozsah problémů Tomáš Rebok, vedoucí divize komunikační infrastruktury ústavu výpočetní techniky.

Jeho pracoviště se stará mimo jiné o knihovnické elektronické služby a katalogy, systémy INET a SUPO, datová úložiště nebo webhosting. Vedle toho funguje na škole celý velký tým centra výpočetní techniky, který pečuje o denní provoz a také vývoj Informačního systému MU, zkráceně ISu.

Podle Tomáše Reboka obnáší zajištění bezpečnosti univerzitních počítačových sítí několik úrovní úkolů: Základem je provoz všech služeb na plně podporovaných a aktuálních systémech, nezbytností je i důsledné řízení přístupu k nim a také stálý monitoring, díky kterému je možné potenciální bezpečnostní problémy odhalovat a také řešit.

Jestli si někdo pod slovním spojením „stálý dohled" představí řadu monitorů s blikajícími čísly jako v nějakém špionážním filmu, není podle slov Jitky Brandejsové z centra výpočetní techniky pečujícího o IS daleko od pravdy. Hlášení o stavu klíčových systémů se skutečně zobrazují na několika monitorech v jedné místnosti. A při plánovaných nárazových zátěžích u nich v konkrétní čas sedí vývojář senior, který je připravený sledovat a případně řešit abnormální chování.

Jen za minulý rok bylo odhaleno a potlačeno asi 82 tisíc pokusů o útok.

„Nejde o to, že by IS zátěž třeba pěti tisíc studentů při startu registrace předmětů nezvládl, ale spíš o kontrolu, jestli někdo nevyvíjí záměrně nadměrnou činnost klikáním, ať už ve prospěch svého studia, nebo aby poškodil systém," přibližuje Brandejsová.

Když má přiblížit nejčastější typy útoků, zmiňuje Tomáš Rebok už jen to, že se nevítaní hosté pokouší univerzitní sítě a v ní aktivní systémy a služby mapovat. Bývá to předzvěst toho, že se útočník bude snažit získat přístup do systému. A mluví také o snahách o prolomení hesla. Cíl je stejný, dostat se dovnitř.

„Zájmy útočníků pak jsou různé. Nejčastěji chtějí získat přístupové údaje k dalším systémům či rozšiřovat softwarové agenty, internetové roboty, v rámci takzvaných botnetových sítí. Tyto následně lze využít pro koordinovaný útok na systémy třetích stran, který je velmi účinný a těžko zastavitelný," říká specialista na informační technologie.

Že jsou vstupy do sítí a jejich ochrana alfou a omegou všeho, o tom mluví i Jitka Brandejsová. „Za nás je nejčastějším problémem odposlechnutí sekundárního hesla. Některými systémy totiž může být posíláno v nezašifrované podobě, a proto je považováno za méně bezpečné. Z toho důvodu IS nedovoluje mít primární a sekundární heslo stejné," zdůvodňuje manažerka vnějších vztahů a marketingu ISu.

Zástupci obou univerzitních ústavů pečujících o bezpečí v IT se shodují, že studenti i zaměstnanci se při práci za počítači chovají zodpovědněji než dříve. Naučili se například neklikat na podezřelé odkazy v e-mailové korespondenci. Základní chyby se ale pořád objevují. Pokud si někdo není jistý, jestli třeba nezadal heslo někam omylem, nebo má podezření, že bylo odhaleno, mají pro něj IT experti jediný vzkaz: Změňte ho.

Kdo by se rád o zabezpečení univerzitních sítí dozvěděl víc, má možnost. Například v ISu je víc informací v sekci Systém, pod odkazem Bezpečnost.

Martina Fojtů