Jak se brání poèítaèové sítì Masarykovy univerzity

30. bøezna 2016 Martina Fojtù

Informaèní systém, e-mailové adresy zamìstnancù, wifi, servery, ohromné množství dat z výzkumù. To všechno se dnes používá nebo vzniká na Masarykovì univerzitì a všechno je potøeba chránit proti zneužití. Univerzita na to má sofistikované systémy a spoustu expertù. Seznamte se s tím, jak pracují.

Každý student nebo zamìstnanec univerzity dennì aktivnì využívá øadu nástrojù a vìtšinou nijak zvláš• nepøemýšlí nad tím, díky èemu fungují. Pøitom je to komplikovaná a pomìrnì nákladný úkol.

„Jen za minulý rok bylo odhaleno a aktivnì potlaèeno asi 82 tisíc pokusù o narušení bezpeènosti infrastruktury univerzity. Jinak øeèeno k takovýmto docela standardním útokùm docházelo prùmìrnì 225krát dennì," naznaèuje rozsah problému Tomáš Rebok, vedoucí divize komunikaèní infrastruktury ústavu výpoèetní techniky.

Jeho pracovištì se starámimo jiné o knihovnické elektronické služby a katalogy, systémy INET a SUPO, datová úložištì nebo webhostingy. Vedle toho funguje na škole celý velký tým centra výpoèetní techniky, který peèuje o denní provoz a také vývoj Informaèního systému MU, zkrácenì ISu.

Podle Tomáše Reboka obnáší zajištìní bezpeènosti univerzitních poèítaèových sítí nìkolik úrovnì úkolù: Základem je provoz všech služeb na plnì podporovaných a aktuálních systémech, nezbytností je i dùsledné øízení pøístupù a také stálý monitoring, díky kterému je možné potenciální bezpeènostní problémy odhalovat a také øešit.

Jestli si nìkdo pod slovním spojením „stálý dohled" pøedstaví øadu monitorù s blikajícími èíslyjako v nìjakém špionážním filmu, není podle slov Jitky Brandejsové z centra výpoèetní techniky peèujícího o IS daleko od pravdy. Hlášení o stavu síových systémù se skuteènì zobrazují na nìkolika monitorech v jedné místnosti. A pøi plánovaných nárazových zátìžích u nich v konkrétní èas sedí vývojáø senior, který je pøipravený sledovat a pøípadnì øešit abnormální chování.

„Nejde o to, že by IS zátìž pìti tisíc studentù pøi startu registrace pøedmìtù nezvládl, ale spíš o kontrolu, jestli nìkdo nevyvíjí zámìrnì nadmìrnou èinnost klikáním, a• už ve prospìch svého studia, nebo aby poškodil systém," pøibližuje Brandejsová.

Když má pøiblížit nejèastìjší typy útokù, zmiòuje Tomáš Rebok už jen to, že se nevítaní hosté pokouší univerzitní sítì a v ní aktivní systémy a služby mapovat. Bývá to pøedzvìst toho, že se útoèník bude snažit získat pøístup do systému. A mluví také o snahách o prolomení hesla. Cíl je stejný, dostat se dovnitø.

„Zájmy útoèníkù pak jsou rùzné. Nejèastìji chtìjí získat pøístupové údaje k dalším systémùm èi rozšiøovat softwarové agenty, tzv. internetové robot}', v rámci takzvaných botnetových sítí. Tyto následnì lze využít pro koordinovaný útok na systémy tøetích stran, který je velmi úèinný a tìžko zastavitelný," øíká specialista na informaèní technologie.

Že jsou vstupy do sítí a jejich ochrana alfou a omegou všeho, o tom mimi i Jitka Brandejsová. „Za nás je nejèastìjším problémem odposlechnutí sekundárního hesla. Nìkterými systém}"totiž mùže být posíláno v nezašifrované podobì, a proto je považováno za ménì bezpeèné. Z toho dùvodu IS nedovoluje mít primární a sekundární heslo stejné/' zdùvodòuje manažerka vnìjších vztahù a marketingu ISu.

Zástupci obou univerzitních ústavù peèujících o bezpeèí v IT se shodují, že studenti i zamìstnanci se pøi prácí za poèítaèi chovají zodpovìdnìji než døíve. Nauèili se napø. neklikat na podezøelé odkaz}"v e-mailové korespondenci. Základní chyby se ale poøád objevují. Pokud si nìkdo není jistý, jestli tøeba nezadal heslo nìkam omylem, nebo má podezøení, že bylo odhaleno, mají pro nìj IT experti jediný výkaz: Zmìòte ho.

Kdo by se rád o zabezpeèení univerzitních sítí dozvìdìl víc, má možnost. Napøíklad v IS je víc informací v sekci Systém, pod odkazem Bezpeènost.

Jestli si nìkdo pod slovním spojením „stálý dohled" pøedstaví øadu monitorù s blikajícími èíslyjako v nìjakém špionážním filmu, není podle slov Jitky Brandejsové z centra výpoèetní techniky daleko od pravdy.