ROZHOVOR

Útočí hlavně automaty

RADAN DOLEJŠ

Více než 95 útoků je vedeno náhodně pomocí botů, říká síťový architekt společnosti Compunet Filip Weber.

Jak vypadá bezpečnost u zákazníka, k němuž jdete prvně?
Velmi často je v tragickém stavu. Mnohokrát není k dispozici rozsegmentování sítě, nejsou udělané WLAN a přístup do sítě má kdokoliv. Firewally mají špatně nakonfigurované nebo jejich nastavení není dotažené do konce. Častou chybou jsou otevřené a zapnuté internetové zásuvky v zasedacích místnostech, kde nechávají návštěvy samotné.

Pozorujete pokusy o pronikání do sítí, které chráníte?
Samozřejmě, poměrně často. Možná víc než 95 procent útoků mají na starosti boty, tedy automaty, které se snaží z nakaženého počítače proniknout do některého připojeného systému. Není to cílený útok, je veden náhodně ze strojů, které byly nakaženy. Pro útočníka je to práce s nejistým výsledkem i ziskem. Takové útoky se snaží probourat do sítě, najít a odeslat třeba databázi účtů a přístupových jmen i hesel. Prvotním cílem je samozřejmě soubor kreditních a debetních karet.

S útoky, kdy by někdo cíleně napadl firmu se záměrem ukrást nebo zničit data, jsem se ještě nesetkal. Ale dějí se.

Jak se vás dotýkají všechny zranitelnosti, které se objevují na routerech a dalším síťovém hardwaru?
Hodně se s tím pereme, je to poměrně častý jev. Když zabezpečujeme síť, na všechen hardware instalujeme poslední známý a zároveň ověřený firmware. Poslední totiž vždy neznamená nejlepší. Zákazníkům doporučujeme používat intrusion prevention systémy, protože mají v sobě integrované ochrany právě proti těmto zranitelnostem. Ty pak ochrání systém i v případě neaktualizovaného firmwaru. Takové systémy jsou ale poměrně drahé, takže ne každý zákazník si je proto koupí.

Ale klientům, kteří mají s námi servisní smlouvu, přes náš dohledový a monitorovací systém instalujeme aktualizované firmwary do sítě automaticky.

Co je pro vás aktuálně největším trendem v bezpečnosti?
Ačkoliv to není novinka, je to BYOD a související systém na správu mobilních zařízení – MDM. Pro českou firmu je MDM ale většinou mimo rozpočet, protože náklady na zavedení MDM se pohybují od jednoho do pěti tisíc korun na zařízení.

BYOD se dá jednoduše mplementovat jen pomocí nástroje pro centrální správu Wi-Fi, který společnosti většinou mají. Je to jednodušší řešení, než dávat zaměstnancům na výběr z několika modelů – žádný totiž nebude pro všechny pracovníky vhodný. Pro správce je proto jednodušší vypustit otázku zjišťování zařízení a soustředit na otázku identifikace a oddělení mobilních zařízení do zvláštní zóny.

S bezpečnostní souvisí další současný trend – SIEM nebo alespoň sběr logů. Firmy si tyto systémy pořizují nejen kvůli požadavkům Zákona o kybernetické bezpečnosti, ale i kvůli řešení vlastních provozních problémů a auditů. ■

FILIP WEBER,
SÍŤOVÝ ARCHITEKT, COMPUNET

> Prvotním cílem útoků je samozřejmě soubor kreditních a debetních karet.