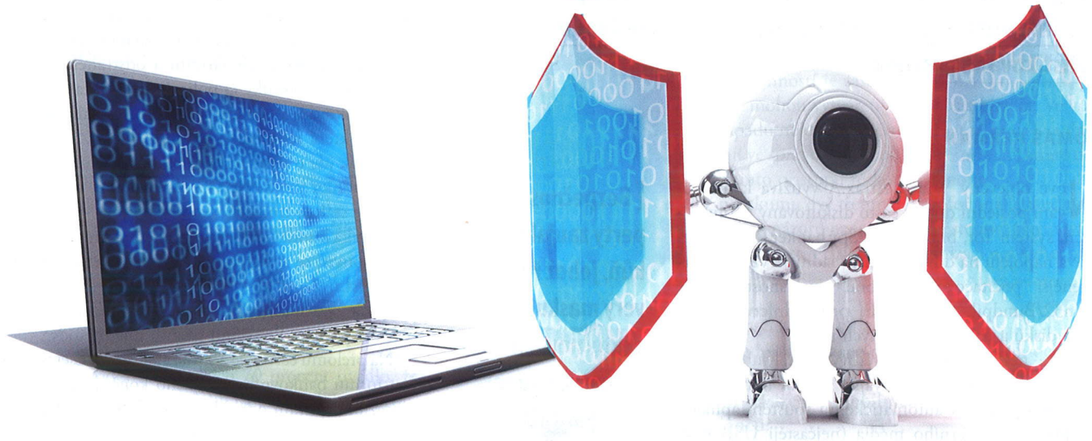
Distribuovaná kybernetická bezpečnost po česku



CZ.NIC nedávno představil projekt distribuované kybernetické bezpečnosti – vyvíjí totiž vlastní router doplněný o speciální software. Vše se přitom děje výhradně v české provenienci a na bázi open source řešení. Směrovač je zatím ještě ve vývoji, takže tento článek objasňuje především pozadí celého projektu a jeho hlavní myšlenky i cíle.

BEDŘICH KOŠATA

Distribuovanou kybernetickou bezpečnost představil CZ.NIC na jaře tohoto roku. V jeho rámci pracují odborníci na vývoji bezpečnostní sondy, která bude schopna analyzovat protékající síťový provoz, identifikovat potenciálně nebezpečné datové toky a reagovat na jejich výskyt.

Sonda bude mít podle tvůrců podobu běžného domácího routeru, bude však v sobě ukrývat výrazně výkonnější hardware, než bývá u těchto zařízení běžné.

Prvotní myšlenka celého projektu byla jednoduchá – najít vhodný způsob, jak přispět ke zlepšení bezpečnosti domácích uživatelů. Jako zajímavá možnost byla identifikována právě ochrana zabudovaná do domácího routeru.

Ten je totiž v naprosté většině případů hlavní branou mezi domácí sítí a internetem, a všechny případné útoky tak musí procházet právě jím. Router je tedy i nejvhodnějším místem pro zamezení možným atakům.

Z této základní myšlenky – chránit uživatele pomocí speciálního softwaru na domácím routeru – pak vyplynuly všechny další vlastnosti a části tohoto projektu.

[Aby šlo uživatele před nebezpečným provozem chránit, je třeba nejdříve vědět, jaký chod vlastně na rozhraní sítě a internetu je.]

Aby bylo možné domácí uživatele chránit před nebezpečným provozem, je třeba nejdříve vědět, jaký chod vlastně na rozhraní domácí sítě a internetu je. Je tedy třeba síťový provoz nejprve analyzovat a na základě získaných informací pak připravit vhodný způsob ochrany.

Analýza aktuálního provozu samozřejmě není jedinou možností, jak data o potenciálních nebezpečích získat – další možností jsou například informace, kterými disponuje český národní CSIRT tým, který sídlí právě v CZ.NIC.

I přesto je ale analýza síťového provozu hlavním zdrojem dat o možných bezpečnostních rizicích. Z toho důvodu začal v rámci projektu vznikat tzv. distribuovaný adaptivní firewall, tedy firewall, který se umí přizpůsobovat novým hrozbám a ke sběru dat používá distribuovanou síť sond.

Součástí firewallu je programové vybavení pro sběr a analýzu dat přímo v domácím routeru, software pro centrální server, který má za úkol sbírat důležitá data z jednotlivých sond, systém pro vyhodnocování získaných dat a vytváření nových firewallových pravidel a systém pro jejich distribuci na zapojená zařízení.

Nutnou podmínkou pro úspěšnost navrhovaného řešení je nutnost vytvoření dostatečně velké sítě sond, která umožní relevantní data sbírat. Z této potřeby vznikla myšlenka spojit sondu s klasickým domácím routerem a nabízet ho za výhodných podmínek koncovým uživatelům, kteří budou ochotni tuto analýzu na rozhraní své sítě dělat.

Jedním z hlavních cílů projektu se tak stal nejen vývoj softwaru pro „distribuovaný adaptivní firewall“, ale také příprava a umístění přibližně 1 000 bezpečnostních sond v sítích koncových uživatelů. Takové množství sběrných bodů by mělo umožnit sběr dostatečného množství dat pro plánované analýzy.

Kromě programového vybavení byl jedním z problémů při přípravě sond výběr vhodného hardwaru. Většina na trhu dostupných domácích routerů je z ekonomických důvodů velice přesně optimalizována právě na předpokládaný provoz a způsob použití a nedisponuje přebytečným výkonem, který by bylo možné bez ztráty rychlosti provozu využít pro analýzu protékajících dat.

Po průzkumu trhu tak přišlo na řadu řešení šité projektu na míru, tedy návrh a výroba vlastního hardwaru.

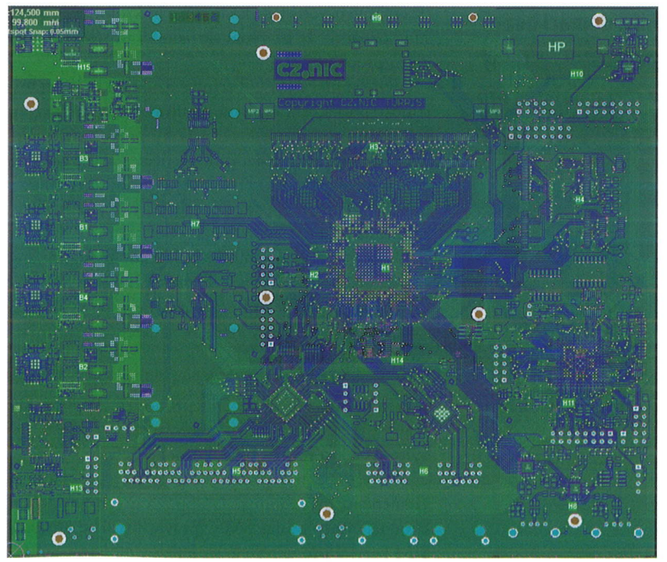
To je ale oblast, ve které nemá CZ.NIC žádné předchozí zkušenosti, a musel tak přistoupit k rozšíření svého vývojového týmu o experty na vývoj hardwaru a zároveň navázal spolupráci s odborníky z Fakulty informačních technologií VÚT Brno, kteří vznikajícímu týmu pomohli s přípravou návrhu hardwaru pro výkonný domácí router.

Ten je dimenzován tak, aby s rezervou zvládl běžný domácí síťový provoz včetně požadované analýzy dat. Obsahuje tak například dvoujádrový PowerPC procesor, taktovaný až na 1,2 GHz a minimálně 2 GB RAM.

Toto zařízení, které se zatím vyvíjí pod jednoduchým kódovým označením „CZ.NIC router“, by se tak mělo stát ústředním bodem projektu, protože v sobě bude spojovat veškeré výsledky práce celého týmu vývojářů – od vlastního návrhu hardwaru přes přizpůsobený operační systém na bázi Linuxu až po síťové sondy pro statistickou analýzu síťového provozu.

Cíle a budoucí plány

Hlavním cílem pro letošní rok je vyrobit tisícovku výše zmíněných směrovačů a začít s jejich distribucí koncovým zákazníkům. V následujícím roce se pak bude zejména vyvíjet další bezpečnostní software, v závislosti na zkušenostech s daty získanými z provozu takto velkého množství zařízení.



Základní deska nově vyvíjeného routeru ryze české provenience

Jak to funguje

Systém označovaný jako distribuovaný adaptivní firewall je v této chvíli ve fázi aktivního vývoje. Jeho součástí je klientská část, která po aktivaci na domácím routeru monitoruje nevyžádané pokusy o přístup do sítě zastavené firewallem a také analyzuje protékající data.

V nich se pokouší odhalit anomálie, které by mohly být příznakem úspěšného útoku nebo již existující nákazy. Výsledky obou zmíněných částí klientského systému se nahrávají na druhou část systému, kterou je centrální server, kde se data dále zpracovávají a porovnávají s výsledky z ostatních sond.

Pokud se systémem některá část provozu označí jako anomální a obsluha systému vyhodnotí danou anomálii jako potenciální útok, připraví pro ni nové pravidlo pro firewall. To se potom formou aktualizace nahraje zpět na všechna zařízení zapojená do sběru dat.

Pro případy, kdy je třeba o dané anomálii získat doplňující informace, je součástí systému také nástroj na spouštění specializovaných „mikrosond“, které je možné formou modulů nahrávat na sledovaná zařízení. Ty pak umožní zaměřit analýzu na konkrétní typ provozu a získat detailnější data o daném jevu.

Jako základ vývoje operačního systému pro CZ.NIC router se použil OpenWrt, který se dále upravuje a rozšiřuje o potřebnou funkcionalitu. Jde například o použití validujícího DNS resoveru Unbound namísto výchozího DNSMasq nebo o výměnu minimalistického SSH serveru Dropbear za OpenSSH. Uživatel si také může sám doinstalovat třeba server pro sdílení souborů v domácí síti nebo bittorrent klienta.

CZ.NIC podle svých slov počítá také s veřejným testováním. Pokud se tedy někdo hodlá jako aktivní člen zapojit do vývoje zde popsaného řešení, měl by sledovat stránky projektu *www.turris.cz*, kde se lze dozvědět více. (pal)

Projekt distribuovaného adaptivního firewallu by se tak měl posunout z oblasti výzkumné do sféry plnohodnotného bezpečnostního nástroje. Výsledky získané z analýzy dat se budou publikovat pro odbornou veřejnost.

Budou také ve formě pravidel pro firewall k dispozici nejen uživatelům „CZ.NIC routeru“, ale také uživatelům komerčních routerů nebo linuxových serverů.

Další úsilí se bude také věnovat vývoji v oblasti operačního systému pro domácí routery, který by chtěl CZ.NIC poskytnout i pro jiné verze. Motivací k tomuto kroku je poměrně stagnující situace na poli domácích smerovačů, kdy například zavádění podpory pro protokol IPv6 nebo zabezpečení DNS pomocí DNSSEC je ze strany dodavatelů těchto přístrojů stále relativně pomalé.

Důležitou otázkou v tomto projektu je ochrana soukromí uživatele – podmínky poskytnutí routeru koncovým uživatelům a sběru dat budou vymezeny smluvně a veškerý software dodávaný s routerem bude uvolněn pod open source licencí, a to vždy před jeho nasazením na samotná zařízení.

Otevřenost řešení

Vzhledem k tomu, že součástí projektu bude také vývoj hardwaru, budou i veškeré výstupy v této oblasti uvolněny pod otevřenou licencí, a bude tedy možné získat kompletní schéma zapojení komponent routeru a podklady pro výrobu desky plošných spojů.

CZ.NIC router se tak řadí do stále rostoucí skupiny otevřeného hardwaru, po bok projektů, jako jsou Raspberry Pi4 nebo Arduino5.

Na rozdíl od zmíněných produktů však jde o hardware pro síťové účely, což zatím není oblast, ve které by byl open hardware příliš obvyklý. ■

Autor pracuje jako vedoucí vývojového týmu CZ.NIC.