

Komentář

Brno 3.5. 2011

McAfee Application Control jako kritická bezpečnostní aplikace v systémech Siemens

Společnost Siemens (divize průmyslové automatizace) potvrdila kompatibilitu softwaru McAfee Application Control se systémy Siemens. McAfee Application může být tím pádem použit jako ochrana proti útokům typu Advanced Persistent Threat, které mohou vést kromě průmyslové špionáže až k sabotážím. Vzpomeňme např. na červa nazvaného Conficker, kterého lze mezi podobné útoky řadit. Známy útok s cílem odcizit data z průmyslových systémů také byl odhalen společností McAfee a dostal název Night Dragon. V žádném z útoků se nejednalo o podružné či nedůležité systémy, cílem byly řídicí systémy turbín v jaderných elektrárnách nebo centrální pulty pro těžbu ropy.

Oba dva útoky spojuje několik nápadných rysů. Vždy byly cílem průmyslové systémy Siemens, které bez dostatečného zabezpečení neměly šanci útokům odolat. Dále bylo potřeba po exploitaci systému (ať už lokální nebo vzdálené) sbírat dodatečná data, spouštět vlastní programy (nebo aspoň programy často užívané pro administraci systémů). V případě použití McAfee Application Control by celý útok selhal ihned po exploitaci, která probíhala například zasíláním podvržených pdf dokumentů. Zneužití samotné zranitelnosti by zabráněno nebylo, ale kód, který by se měl na takto zranitelném systému spustit, by byl jednoduše zablokovan a celý útok by přišel vniveč.

McAfee Application Control funguje na bázi dynamického whitelistingu. Při instalaci na čistý stroj si Application Control oskenuje současné softwarové vybavení, které v budoucnu povolí spustit, ale nové programy blokuje, a to včetně těch, které jsou zavedeny přímo do paměti pomocí zranitelnosti přetečení zásobníku. Aby byl whitelisting opravdu dynamický, povolíme pouze několika aplikacím měnit zbytek programového vybavení, resp. whitelist (aplikace, které se starají o aktualizace). Přímočarý a robustní princip Application Control zaručuje jednoduché nasazení, minimální nároky na výkon a velmi vysokou úroveň zabezpečení. Systémy společnosti Siemens budou i nadále cílem útoků, proto bylo potřeba vybrat trvalé a účinné řešení. Zároveň Siemens světu ukázal, že nebere bezpečnost svých systémů na lehkou váhu.

Robert Šefr, IT Security Consultant, COMGUARD a.s.