Vážené čtenářky, vážení čtenáři,

Pat Gelsinger, výkonný ředitel společnosti VMware a bývalý vysoký manažer Intelu, nedávno zpochybnil současnou praxi fungování zabezpečení.

Bezpečnostní trh se podle něj v pohledu na kyberbezpečnost mýlil, když přijal za své model, kdy se snaží komplexně chránit technologie a řešení. Gelsinger tak zpochybňuje dosavadní praxi, kdy se vybuduje obecná IT infrastruktura a poté se do ní nasazuje řada bezpečnostních systémů chránících organizaci proti každodennímu přílivu hrozeb.

Když se prý podíváte na své bezpečnostní výdaje, jasně vidíte, že stále více utrácíte, a přitom i více ztrácíte. Podle Gelsingera je proto nutné nalézt model, kdy při použití méně zabezpečovacích řešení získáte větší ochranu.

A jak to lze podle něj vyřešit? Nový přístup by se totiž už neměl zaměřovat na pronásledování bezpečnostních hrozeb, ale naopak radikálně snížit možnosti útoku.

Budovat by se mělo prostředí, které už má vnitřní bezpečnost a je navržené tak, aby pracovalo správně bez možnosti rizik – jde tedy vlastně o myšlenku bezpečnosti vestavěné přímo do všech produktů.

Podle Gelsingera lze díky těmto mechanismům v IT infrastruktuře eliminovat většinu složitostí a nasazování řady senzorů, agentů či speciálních bezpečnostních boxů.

Nakolik je tato myšlenka v praxi uskutečnitelná, sice není v současnosti úplně jasné, nicméně ukazuje se, že tlaky na změnu podoby současného zabezpečení výrazně sílí, přičemž podporu pro ni začínají vyjadřovat stále významnější špičky technologického světa.

Jednou z prvních vlaštovek může být třeba změna v přístupu k vývoji aplikací – model DevSecOps, o němž v tomto vydání Security Worldu podrobně informujeme, totiž předpokládá výrazné zapojení bezpečnosti už při samotném vývoji programů, což by mělo vést právě k výrazně nižším hrozbám v této oblasti.

S přáním příjemně stráveného podzimu třeba i nad stránkami nejnovějšího Security Worldu přeje

Pavel Louda
vedoucí projektu

Obsah