Zero trust koncept pro správu identit

Podnikové IT i celá infrastruktura se rychle mění, přičemž společnosti stále častěji využívají externí správu svých systémů a mnoho z jejich aplikací již běží v externím cloudu.

Tato transformace bude v budoucnosti stejně významná, jako byl přesun klasické infrastruktury serverů do světa virtualizace, bez níž si v posledních letech nedokážeme představit základní fungování IT.

Podporou této změny bude potřeba nových technologických dovedností, zejména v oblasti bezpečnosti a zabezpečení přístupu. Společnosti musejí neustále přehodnocovat způsoby reorganizace IT, což pro ně znamená využívání nových poskytovatelů služeb, nástup nových týmů a budování nových oddělení nebo třeba transformace cloudu v kombinaci s návrhem a implementací nových procesů návrhu zabezpečení.

Úloha bezpečnostních týmů v provozním modelu cloudu je přitom klíčová, protože nikdo jiný nemůže zabezpečit provoz včetně aplikací a správy infrastruktury. Pokud se chtějí společnosti zaměřit na zabezpečení dat a správu identit, musejí zavést principy nulové důvěry a zároveň vyvinout specifické bezpečnostní strategie pro zabezpečení koncových bodů, aplikací a infrastruktury.

Když se ohlédneme zpět, v typickém on-premise modelu dnešní virtuální infrastruktury začíná „IT Security Playbook“ zabezpečením a správou hesel v trezoru a monitorováním privilegovaných relací nad operačními systémy, databázemi a síťovými prvky. Většina organizací vyřešila počáteční problémy s nasazením správy privilegovaného přístupu tím, že vsadila na přístup založený na ochraně perimetru, případně pomocí ZTNA přístupu. Pro většinu podniků ale stále zůstává výzvou, jak vyřešit otázky úniku dat, laterálního pohybu útočníka na síti nebo šifrování citlivého provozu, když uživatelé přistupují z více míst a z nespravovaných koncových bodů.

Mnoho nejrůznějších produktů poskytuje na začátku jednoduchou možnost integrace, následně ale často zvyšují složitost zabezpečení specializovanými službami s dalšími licenčními náklady. Existují ale výjimky, například platforma Sectona, která spojuje prvky pro zabezpečení privilegií a je vyvinuta od základu pro snadné používání v rámci integrovaného řešení pro správu privilegií se zaměřením na automatizaci, jednoduchost a nenáročnost obsluhy.

Projekty správy oprávnění obvykle začínají fází zjišťování aktiv sledovaných v několika systémech CMDB, tabulkách a souborech. Tradičními přístupy při zjišťování zůstává buď využití zjišťování AD, nebo skenování sítě. Funkce Continuous Discovery paltformy Sectona je výchozím bodem pro poskytování dynamického přístupu koncovým uživatelům bez lidského zásahu. Sectona Continuous Discovery využívá integraci s hlavními poskytovateli cloudových služeb včetně AWS a Azure, VMWare vSphere a Hyper-V pro privátní cloud, SNMP pro síťová zařízení a skenování sítě. Druhá část procesu Discovery poskytuje přehled o privilegovaných účtech, přičemž jsou podporovány účty napříč serverovou infrastrukturou systémů Windows a Unix, Microsoft SQL, Oracle databází a Oracle MySQL a pracovních stanic se systémem Windows. Funkce Discovery může automaticky dělat úlohy pro vyhledávání nových zdrojů ve vícecloudových prostředích s více lokalitami spolu s přidruženými privilegovanými účty.

Platforma Sectona Security Platform se integruje například s cloudovými platformami pro správu identit a přístupu, se systémy založenými na SAML nebo s poskytovateli cloudových služeb MFA pro ověřování, aby bylo možné ověřit identitu uživatelů přistupujících z libovolného místa a zajistit bezpečný přístup přes prohlížeče s VPN nebo bez ní. Platforma Sectona Security Platform poskytuje technologii zabezpečeného vzdáleného přístupu pro přístup ke sdíleným prostředkům v prostředí společnosti nebo cloudu pomocí libovolného webového prohlížeče. Sectona poskytuje přístup k iniciaci a monitorování relací v prohlížeči, který umožňuje přístup k RDP, SSH, aplikacím, FTP, SFTP s jednotným privilegovaným přihlášením a správou relací. Automatizované vkládání pověření pomocí Sectona Vault a implementace Zero Standing Privileges pro vzdálené uživatele s dynamickými možnostmi provisioningu snižuje riziko krádeže pověření nebo zneužití zprostředkovaných privilegií.

Díky rozsáhlým auditovatelným funkcím také budete mít pod kontrolou, kdo má přístup k informacím. Organizace tak při řešení správy oprávnění mohou pracovat s integrovaným, škálovatelným a zdrojově efektivním přístupem při správě oprávnění, bez skrytých nákladů na zdroje nebo licencování.