

Od detekce zranitelností k vizualizaci cest průniku

V dnešním dynamickém kybernetickém prostředí již nestačí pouze pasivně čekat na útok a následně na něj reagovat. Klíčem k efektivní obraně je proaktivní správa útočné plochy (attack surface management).

Pavel Škorpil

Security Specialist v IS4 security

Společnost Bitdefender ve své platformě GravityZone posouvá koncept analýzy rizik na zcela novou úroveň, kdy kombinuje tradiční monitoring endpointů s pokročilými technologiemi pro skenování vnějšího perimetru, monitoringem cloudu a síťovou analýzou. To vše koreluje navzájem, vyhodnocuje pomocí AI a vizualizuje uživateli možné cesty průniku do sítě.



Základní pilíř: Risk management nad endpointy

Základem každé analýzy rizik v ekosystému Bitdefender je modul Risk Management. Ten neustále monitoruje a vyhodnocuje stovky faktorů přímo na koncových zařízeních. Nejde jen o detekci malware, ale především o identifikaci chybných konfigurací operačního systému a přítomnost zranitelných aplikací, které by útočník mohl zneužít. Tento modul poskytuje jasně prioritizovaný seznam rizik, která jsou rozdělena do tří hlavních kategorií:

- Chybné konfigurace – například vypnuté bezpečnostní funkce, slabé politiky hesel nebo nebezpečná nastavení síťových protokolů.

- Zranitelnosti aplikací – detekce neaktualizovaného softwaru s veřejně známými zranitelnostmi (CVE).
- Lidské riziko – analýza chování uživatelů, jako jsou používání nezašifrovaných webů nebo opakované infekce, které indikují potřebu školení.

Pohled očima útočníka

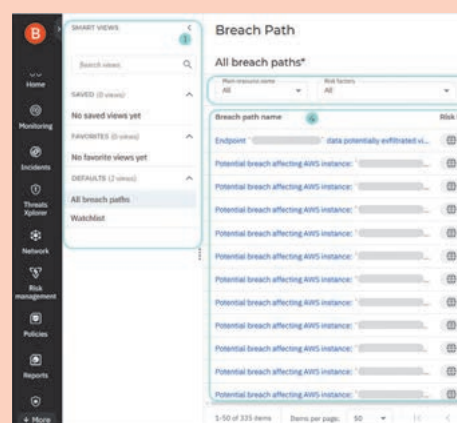
Zatímco klasický agent na endpointu hlídá zařízení samo o sobě, addon External Attack Surface Management (EASM) se dívá na vaši organizaci zvenčí – z internetu. V dnešní době, kdy se hranice firemní sítě díky cloudu a vzdálené práci stírají, je tento pohled zcela kritický. EASM automaticky vyhledává a mapuje veškerá aktiva vystavená do internetu, o kterých IT oddělení často ani nemusí vědět (tzv. shadow IT). Identifikuje zapomenuté subdomény, otevřené porty na firewallech nebo expirované SSL certifikáty. Tím, že Bitdefender neustále skenuje vnější perimetr, dokáže včas varovat před novými vektory útoku dříve, než je stihnou zneužít automatizované skenery útočníků.

Hlubková viditelnost zranitelností

Pro komplexní analýzu rizik je nezbytné rozumět i tomu, co se děje „mezi“ zařízeními. Zde nastupují síťové sondy v rámci XDR (Extended Detection and Response). Běžně síťová sonda analyzuje provoz v reálném čase a hledá anomálie, které senzory na agentech nemusejí zachytit. Síťová sonda může také skenovat zranitelnosti, jež doplňují data z endpointů o pohled na zařízení, na něž nelze instalovat agenty (např. IoT zařízení, tiskárny nebo starší průmyslové systémy).

Breach Path Analysis

Nejvýznamnější inovací, která aktuálně přichází do bezpečnostní platformy Bitdefender GravityZone je funkce Breach Path. Tato technologie představuje revoluci ve způsobu, jakým bezpečnostní týmy interpretují rizika. Namísto pouhého seznamu stovek izolovaných zranitelností a varování dokáže Breach Path tyto informace propojit. Algoritmus analyzuje data z endpointů, síťových sond a EASM, aby vytvořil grafickou vizualizaci pravděpodobných cest, kterou by útočník mohl postupovat.



Shrnutí

Bitdefender GravityZone dávno není „jen“ antivirus. Je to komplexní platforma pro řízení rizik, která propojuje vnitřní stav zařízení, vnější viditelnost a síťový kontext. S příchodem funkcí jako EASM a Breach Path získávají firmy do rukou nástroje, které dříve byly dostupné pouze pro velké SOC týmy. Výsledkem je dramatické snížení útočné plochy a schopnost prioritizovat nápravná opatření tam, kde mají největší dopad na bezpečnost celého podniku.