Zabezpečujete mobilní zařízení, nebo je jen spravujete?

Ještě před několika lety se přístup do sítě ze zařízení ve vlastnictví zaměstnanců zaměstnavatelům nelíbil, byť to bylo například jen k firemní poště. Dnes, částečně díky pandemii covidu a práci na dálku, se ale používání osobních zařízení pro práci stává v podnikové sféře standardem.

PAVEL ŠKORPIL

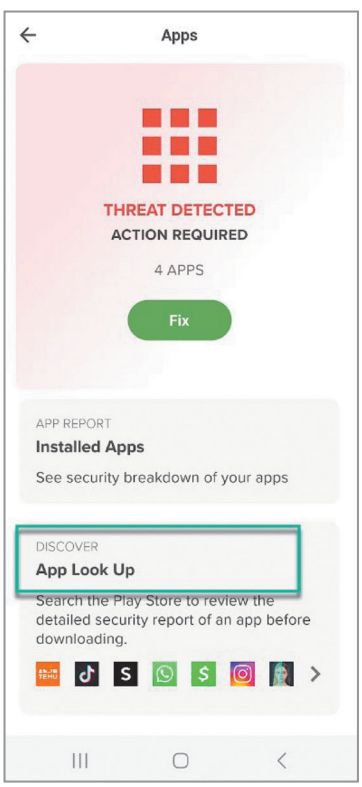
S tím se ale zvyšují i rizika, když zaměstnanci používají aplikace jako např. Office 365, G Suite, JIRA a Salesforce ze svých osobních zařízení, a to i v případě, že nepracují z domova, ale jsou v kanceláři. Tato osobní i firemní zařízení jsou také běžně používána pro vícefaktorovou autentizaci (MFA). Dnes se zařízení používají k ověření identity jednotlivce, tak aby pracovník získal přístup k firemním datům mimo tradiční perimetr společnosti.

Mobilní zařízení jsou tak dnes přímo spojena s identitou jednotlivce. A díky tomu zde rychle roste prostor pro kyberzločince, kteří díky tomu, že dnes se stírá hranice mezi zařízením a daty, mají k dispozici celou škálu podnikových informací, jež jsou zralé ke krádeži. Výsledkem je, že protivníci vyvíjejí nové taktiky a využívají více kanálů k phishingovým útokům, přičemž mobilní zařízení jsou opět zadními vrátky. Kyberzločinci se cíleně zaměřují na uživatele mobilních řešení, protože poskytují větší přístup k podnikovým datům více než kdy jindy a jsou také mnohem méně chráněna než běžná koncová zařízení.

Starší nástroje kontroly zabezpečení a správy, jako je například správa mobilních zařízení (MDM), jsou dnes již nedostatečné, pokud jde o účinné odhalování a řešení pokročilých hrozeb. MDM je, jak už název napovídá, nástroj pro správu.

Bitdefender GravityZone Security for Mobile

S vývojem technologií, které řeší nové výzvy a potřeby, přinesla moderní mobilní éra novou kategorii zabezpečení, jež pomáhá bojovat proti aktuálním hrozbám. První publikovaná zmínka o této kategorii bezpečnostních řešení se objevila pod názvem



Mobile Advanced Threat Defense (MATD) ve zprávě Gartner 2014 Hype Cycle for Enterprise Mobile Security. V té době byla MATD považována za podmnožinu trhu pokročilé ochrany proti hrozbám (ATD). Mobile Threat Defense se však brzy stala samostatným trhem a již v témže roce se objevila Mobile Threat Defense v prezentaci na summitu Gartner EMEA IT Infrastructure and Operations Management Summit.

Ochrana před mobilními hrozbami – Bitdefender GravityZone Security for Mobile je komplexní řešení mobilního zabezpečení s technologií Mobile Threat Defense, která zabraňuje mobilním hrozbám a detekuje je napříč zařízeními, sítěmi a aplikacemi. Ochrana využívá různé techniky, jako jsou strojové učení (ML) a analýza chování k odhalování hrozeb, prověřování aplikací a správa zranitelností daného zařízení. Mobile Threat Defense a MDM mají společný cíl – chránit společnosti před mobilními hrozbami – Security for Mobile je rozšíření ochrany o pokročilé technologie zabezpečení pro správu mobilních zařízení.

GravityZone Security for Mobile představuje proaktivní způsob ochrany mobilních zařízení před útoky a hrozbami. Mobile Threat Defense funguje jako komplexní poplašný systém, který nepřetržitě skenuje zařízení a chrání je před hrozbami. Pokud zařízení není zabezpečené – jestliže dojde k útoku nebo se vyskytne zranitelnost, například nezáplatovaný software – uživatel i správce IT společnosti budou informováni.

GravityZone Security for Mobile skenuje několik druhů útoků, jako jsou například útoky typu SSL-stripping, Man in The Middle, phishing, podvodné sítě, malware a další. Strojové učení zase odhalí a zabrání mobilním hrozbám napříč zařízeními, sítěmi, phishingem a útoky škodlivých aplikací. V zařízení bude nasazeno komplexní řešení bezpečnosti. Pomocí řešení Security for Mobile bude bezpečnostní správce mít větší kontrolu nad zásadami potřebnými ke splnění přísných požadavků na zabezpečení a dodržování vnitřních předpisů. Organizace využívající řešení GravityZone Security for Mobile by měly prezentovat zásady ochrany osobních údajů, tak aby zaměstnanci snáze pochopili, jak je s daty nakládáno a že jejich zařízení jsou chráněna, aniž je narušeno jejich soukromí.

Využití nástrojů pro Mobile Threat Defense a MDM ve vzájemné shodě přináší některé další výhody. Například jakmile je jednou v MDM zaregistrováno mobilní zařízení, jsou na něm aplikovány zásady a jsou zpřístupněny podnikové zdroje dat, může správce organizace bezpečně nasadit na zařízení pokročilou ochranu Security for Mobile, přičemž pro zaměstnance to bude představovat minimální omezení, která by zasahovala do jejich každodenní produktivity.

Autor je Security Specialist