10 Znakov, že je čas na prehodnotenie Vašej ochrany endpointov

Pretrvávajúci trend úspešných kybernetických útokov dokazuje, že postupy kybernetickej bezpečnosti nedržia krok s modernými hrozbami. Je vaša organizácia dobre chránená, alebo s rizikom žije na dlh? Tu je desať znakov, ktoré vám pomôžu určiť, či je vaše zabezpečenie koncových zariadení pripravené čeliť hrozbám, alebo je čas ísť do dôchodku.

BlackBerry Cybersecurity

1. Stále používate bezpečnostné produkty založené na signatúrach

V minulosti bolo možné nový škodlivý softvér individuálne detegovať, kategorizovať a zablokovať bezpečnostnými spoločnosťami. Škodlivé súbory boli identifikované podľa ich jedinečného hash súboru, tzv. signatúry, a ich spúšťanie bolo obmedzené bezpečnostnými riešeniami založenými na signatúrach. Obrovský počet jedinečných hrozieb generovaných v súčasnosti výrazne znižuje účinnosť prístupu k bezpečnosti založeného na podpisoch.

2. Vaše mobilné zariadenia sú zraniteľné

Zamestnanci pravidelne pristupujú k pracovným zdrojom pomocou smartfónov, mobilné zariadenia sa tak stávajú hlavným cieľom phishingových útokov. Až 45% organizácií sa stalo obeťou útoku, zahŕňajúc mobilné zariadenia, ktorý viedol k strate údajov, výpadkom alebo iným negatívnym dôsledkom. Mobilné zariadenia sú tiež hlavnými kandidátmi na únik údajov, čo môže viesť k porušeniu právnych predpisov a pokutám.

3. Stále vykonávate pravidelné scanovanie koncových zariadení a serverov

Staršie AV riešenia sa spoliehajú na skenovanie systému na zistenie zdroja malware. Tieto kontroly môžu byť plánované alebo na vyžiadanie, alebo sa vyskytujú po aktualizáciách signatúr. Bez ohľadu na to, kedy k nim dochádza, ich negatívny vplyv na výkon systému je nepopierateľný. Ak vaše bezpečnostné riešenie stále vyžaduje skenovanie systému, možnoje čas na aktualizáciu.

8.47 million new malware detected per month.[2]

4. Vaše nové PC sa zdá byť pomalé

Mnohé organizácie zavádzajú viacúrovňový model zabezpečenia. V priebehu času, nahromadenie mnohých bezpečnostných nástrojov môže zaťažovať systémové zdroje a negatívne ovplyvniť výkon systému. Pomalé PC môžu byť jedným zo znakov, že je čas prehodnotiť vašu stratégiu koncových bodov.

5. Chýba Vám efektívna ochrana offline režimu

Koncové body sú zraniteľné v režime offline aj online, takže je dôležité mať zabezpečenie aj vtedy, keď nie ste pripojení aby ste zabránili infikovanému flash disku alebo neoprávnenému používateľovi poškodeniu zariadenia.

6. Trávite príliš veľa času spravovaním svojej AV

Každá minúta, ktorú váš IT tím stráví správou AV riešenia je minúta, ktorá je ukrátená o hlavnú produktivitu podniku alebo o strategické projekty, ktoré by mohli proaktívne posilniť vašu obranu. Ak je vaše súčasné riešenie časovo náročné pre vašich technických špecialistov, je čas zvážiť nové možnosti.

7. Trávite priveľa času reagovaním na falošné upozornenia

Tak ako sa vyvíjali nové techniky identifikácie škodlivého softvéru, vyvíjal sa aj počet falošne pozitívnych nálezov hlásených novými detekčnými metódami. Ak identifikácia založená na správaní, sandboxing, hostiteľská prevencia vniknutia a filtrovania URL/reprezentácie sú príliš náročné na Váš čas, je čas na zmenu.

8. Vidíte medzery vo Vašej endpoint stratégii

Vaša stratégia pre koncové body nepokrýva staršie zariadenia, alebo nezahŕňa a dostatočne nepodporuje mobilné zariadenia, IoT a OT systémy. Vaše súčasné riešenie má obmedzené alebo žiadne možnosti škálovania na nové a vznikajúce technológie, čo vás robí zraniteľnými voči budúcim inováciám.

9. Vaša stratégia zabezpečenia koncových bodov je úplne reaktívna

Spolieha sa vaša stratégia koncových bodov do veľkej miery na akcie, ktoré sa vyskytnú po úspešnom narušení? Ak vaše súčasné riešenie koncových bodov nedokáže odhaliť škodlivý softvér núteného dňa alebo nevie ponúknuť proaktívnu stratégiu určenú na prevenciu narušenia, je čas zvážiť alternatívne riešenia.

10. Musíte aktualizovať operačný systém aby sa prispôsobil vášmu AV

V niektorých prípadoch sú kritické podnikové systémy uzamknuté na konkrétny operačný systém z technických dôvodov a nie je možné ich aktualizovať. Výber vhodného bezpečnostného riešenia, ktoré beží na mnohých systémoch (starých aj nových) by mohlo vašej organizácii ušetriť peniaze a zároveň zjednodušiť vaše bezpečnostné opatrenia.

Ak niektorý z vyššie uvedených bodov opisuje stav vašej súčasnej stratégie zabezpečenia koncových bodov, môže to znamenať, že je čas na nový prístup. CylanceENDPOINT, poháňaný umelou inteligenciou Cylance® AI, poskytuje inteligentné, automatizované zabezpečenie, prevenciu hrozieb a ochranu pred pokročilými kybernetickými hrozbami pre všetky koncové body.

Viac informácií nájdete na adrese www.blackberry.com/protect.

[1] Verizon Mobile Security Index 2022

[2] 12 Sept 2023, AV-Test, Total Malware

BlackBerry Cybersecurity

8823 | 231103