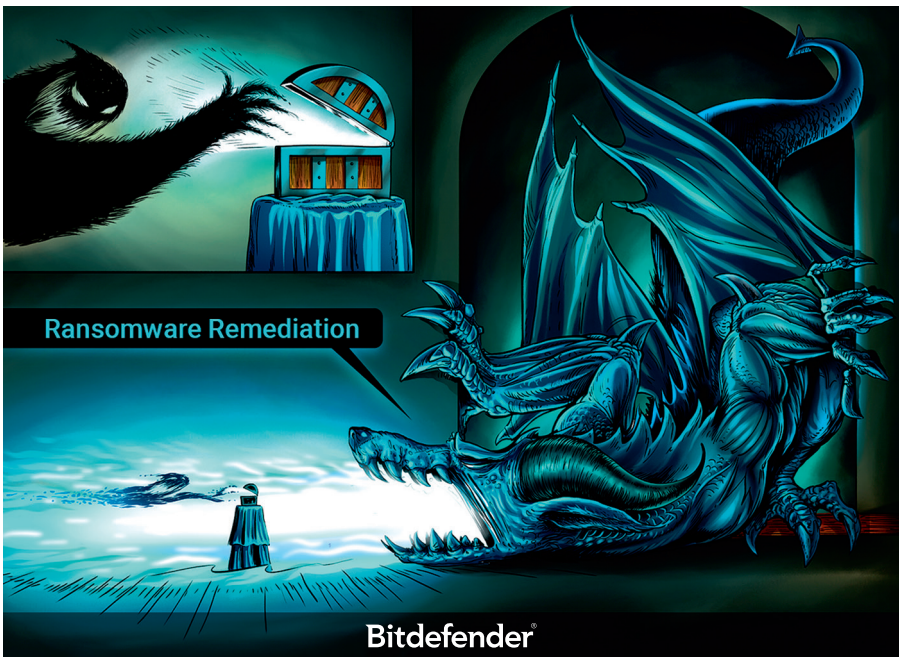
Existuje nějaká pojistka proti ransomware útokům?

Poznejte Bitdefender Ransomware Remediation funkci, která vám dodá bezpečí.



Byli jste obětí vyděračského ransomware útoku? Nebo znáte firmu či instituci, která byla napadena vyděračským zašifrováním dat a jejíž IT infrastruktura byla vyřazena na několik dnů či týdnů? Pokud ano, jistě se vám vybaví otázka: „Dá se proti těmto útokům účinně bránit?“

Na tuto otázku existuje krátká i dlouhá odpověď, ovšem než si na ni odpovíme, je potřeba se zamyslet nad dnešní klasickou antivirovou ochranou, která, jak se dnes bohužel ukazuje, na tuto výzvu sama opravdu nestačí. Proč je tomu tak? Pojďme si to ukázat na jednoduchém příkladu…

Pokud vaše organizace používá například sdílené složky, ačkoliv na daném počítači máte pravděpodobně nainstalovaný klasický antivir, tento agent v absolutní většině případů běžných výrobců neochrání proti útoku z jiné stanice, vedeném například z IoT zařízení, nebo jiné stanice, která není chráněná. Například může jít o zkompromitovanou síťovou tiskárnu, IP kameru nebo stanice se starším OS, z níž je takovýto útok veden a pro kterou například není dostupná podpora od výrobce antiviru.

V takovém případě jednoduše útočník začne útočit v rámci sítě z těchto nechráněných strojů a zašifruje všechna dostupná data na sdílených složkách serveru či stanice, která je nedostatečně chráněná klasickým antivirem. Pokud používáte běžné antimalware řešení, tomuto útoku nezabráníte, protože klasický AV agent nerozpozná legitimní šifrování od nelegitimního šifrování, neboť nedovede zkontrolovat dění na nechráněném zařízení, odkud je útok v rámci sítě veden.

Existuje nějaká technologická pojistka, která vám dodá bezpečí a ochranu a umí tato data vrátit?

Bitdefender se nad touto tematikou zamyslel a vyvinul vlastní sofistikovanou ochranu proti zašifrování dat. Tato technologie vytváří speciální oddíl na disku každé stanice, kam se průběžně zálohují legitimně i nelegitimně šifrovaná data jako například v případě podezřelého šifrování souborů, iniciovaného třeba i z jiných nechráněných stanic. V takovém případě totiž Bitdefender GravityZone BEST klient (od verze ELITE nebo ULTRA) vytvoří preventivně stínovou kopii právě šifrovaných dat za účelem rychlé obnovy. V případě potřeby lze jednoduše veškerá data jedním klikem obnovit zpět. Důležité je přitom, že k této záloze má přístup pouze Bitdefender BEST klient a administrátor Bitdefender GravityZone. Proč je to důležité? Protože velmi často útočníci mažou klasické zálohy, na které se dostanou pomocí získaných administračních práv daného OS. Na tento chráněný oddíl ovšem nevidí ani OS, jen Bitdefender BEST klient. Jde o proprietární vlastní Bitdefender technologii, která v kombinaci s mnohavrstvou Bitdefender GravityZone ochranou umožňuje nejvyšší možnou ochranu vašich firemních či osobních cenných dat. Díky jejímu nasazení můžete zamezit mnohamilionovým ztrátám z výpadku provozu IT a zbytečným finančním škodám, které ransomware útok často stojí.

Dalším slabým článkem mnoha IT infrastruktur v boji proti ransowaru bývá virtualizace

Zamysleme se nad tím, jak chrání (nebo lépe řečeno nechrání) běžné antimalware řešení virtualizovaný stroj… Například pokud používáte VMware s NSX nebo vShield rozhraním, bohužel toto rozhraní umožňuje oskenovat běžnému antiviru pouze soubory na disku (filescan only). Když je ovšem již útočník v paměti napadeného stroje, nezanechá žádnou stopu na disku (fileless attack), a tím pádem takové antivirové řešení vůbec nechrání proti případnému útoku vedenému z paměti virtualizovaného stroje. Proto je potřeba nasadit řešení, jež používá lehké klienty, které umějí ochránit i paměť, registry a běžící služby na virtualizovaných strojích a nespoléhat se na ochranu, která používá pouze vShield nebo NSX přístup. Bitdefender GravityZone právě z tohoto důvodu chrání všechny běžné virtualizační platformy lehkými agenty bez kompromisů na výkon a bezpečnost.

Více o řešení Bitdefender se dozvíte na www.bitdef.cz.