Obrana proti ransomvéru od spoločnosti Cisco: Držte ransomvér v šachu

Čo keby ste mohli zostať lepšie zabezpečení pred ransomvérom aj napriek tomu, že by sa pokúsil o preniknutie? Iba spoločnosť Cisco vám poskytuje bezpečnostné produkty a architektúru, ktoré vám pri tom pomôžu.

Prehľad

Súbory a informácie sú z hľadiska chodu organizácie nevyhnutné. Nutnosť udržiavať tieto informácie – a produktivitu vašej organizácie – v neporušenom a zabezpečenom stave je nespochybniteľná.

Príde však ransomvér, škodlivý softvér alebo malvér, ktorý v počítači jednotlivca alebo organizácie zablokuje informácie, ako sú dokumenty, fotografie a hudba. Prístup k týmto súborom uvoľní až po zaplatení poplatku – výkupného. Po zaplatení sa tieto súbory odomknú a používateľ k nim opäť získa prístup. Bez vhodných prostriedkov obrany môže ransomvér zmeniť organizáciu na skupinu ľudí, ktorí pracujú s perom a papierom, a spôsobiť tak značnú škodu.

Ransomvér sa obvykle rozposiela prostredníctvom kampaní škodlivých kódov, škodlivých reklám (infikovaných reklám na webovej stránke, ktoré môžu šíriť malvér), softvéru zameraného na neoprávnené získavanie údajov (podvodných e-mailov, ktoré sa vydávajú za dôveryhodné), alebo nevyžiadaných správ. Skutočná infekcia sa môže spustiť vtedy, keď niekto klikne na prepojenie alebo prílohu v podvodných e-mailoch. K infikovaniu môže dôjsť aj vtedy, keď používatelia navštevujú stránky so škodlivými reklamami, ktoré automaticky infikujú počítače.

Zoznámte sa s riešením Cisco® Ransomware Defense. Znižuje riziko výskytu infekcií spôsobených ransomvérom vďaka vrstvenému prístupu, a to od vrstvy DNS až po koncový bod k sieti, e-mailu a webu. Dodávame riešenia integrovanej obrany pomocou architektonického prístupu. Ide o spojenie dokonalej viditeľnosti a maximálnej citlivosti voči ransomvéru.

Výhody

- **Zníženie rizika výskytu ransomvéru,** takže sa môžete trvalo sústrediť na chod svojho podnikania
- **Získanie okamžitej ochrany** so zabezpečením, ktoré dokáže zablokovať hrozby ešte predtým, ako sa pokúsia zakoreniť v systéme
- **Získanie bezkonkurenčnej viditeľnosti a citlivosti** zabezpečených prostredníctvom architektonického prístupu od vrstvy DNS do siete až ku koncovému bodu
- **Zabránenie postrannému šíreniu malvéru** vďaka silnej segmentácii siete
- **Získanie výsledkov špičkového výskumu hrozieb realizovaného členmi tímu Talos** a informácií týkajúcich sa ransomvéru

Rýchlo rastúca, výkonná hrozba

Tento rok je rokom ransomvéru. A ukazuje sa, že je skutočne ziskový. Ransomvér sa rýchlo stal najvýnosnejším typom malvéru v histórii.

FBI uviedla, že je na najlepšej ceste k tomu, aby sa stal trhom s ročným výnosom vo výške 1 miliardy dolárov. Výskum tímu Talos spoločnosti Cisco ukazuje, že jediná ransomvérová kampaň dokáže vytvoriť ročný zisk 60 miliónov dolárov. Ransomvér si získava toľko pozornosti, že sa o ňom hovorilo už aj v televíznych programoch.

Útočníci disponujú dostatkom finančných prostriedkov a chcú naďalej pokračovať v inovácií jednotlivých prvkov ransomvéru, čím sa zvýši jeho zákernosť. Domnievame sa, že schopnosť ransomvéru samostatne sa šíriť s cieľom zablokovať veľké časti podnikových sietí sa zdokonalí. Tým by došlo k účinnej porážke funkčnosti podnikových IT systémov, ktorá by ich vrátila späť do 70-tych rokov.

Súčasné reakcie na ransomvér sa zvyknú týkať iba jednobodových produktov. Je nutné, aby sa vzhľadom na rôzne vektory, na ktoré sa zameriava s cieľom postupovať v šírení infikovania, zvážila možnosť zavedenia prístupu na vyššej architektonickej úrovni.

Tento prehľad riešení sa zameriava na rôzne vektory a metódy, ktoré útočníci používajú. Obranné systémy musia v prípade, že dôjde k výskytu infekcie, zabezpečiť e-mail aj web, musia zablokovať prístup k škodlivej infraštruktúre na internete, zastaviť všetky ransomvérové súbory, z ktorých je celý až do koncového bodu vytvorený, zablokovať používané výzvy príkazov a riadenia a zabrániť ľahko dostupnému postrannému postupu ransomvéru.

Čo si kúpiť

Cisco Ransomware Defense združuje všetky potrebné časti bezpečnostnej architektúry Cisco určené na riešenie zložitého problému, ktorý so sebou ransomvér prináša. Môžete sa rozhodnúť pre všetky časti, alebo si vybrať tie, ktoré spĺňajú potrebu okamžitého zabezpečenia.

Ransomware Defense sa skladá z týchto súčastí:

- Cisco Umbrella – blokuje hrozby vo vrstve DNS, a to ďaleko od vašej siete
- Cisco Advanced Malware Protection (AMP) for Endpoints – blokuje postup súborov ransomvéru na koncové body
- Cisco Email Security – riešenie v rámci cloudu aj podnikových sietí, ktoré zastaví správy zamerané na neoprávnené získavanie údajov a nevyžiadané správy, ktoré sa snažia roznášať ransomvér

- Advanced Malware Protection je možné okamžite pridať do produktov zabezpečenia e-mailu prostredníctvom získania jednoduchej licencie na statickú a dynamickú analýzu (izolovaný priestor) neznámych príloh, ktoré prechádzajú bezpečnostnou bránou Cisco na ochranu e-mailov
- Cisco Firepower™ next-generation firewall (NGFW), ktorý blokuje prenos výziev príkazov a riadenia a prípadné škodlivé súbory prechádzajúce sieťou
- Cisco ISE cez sieť Cisco dynamicky segmentuje vašu sieť, takže zabraňuje postrannému šíreniu ransomvéru

Vďaka riešeniu Ransomware Defense môžu organizácie používať svoju sieť ako nástroj, ktorý pomáha zadržať šíriaci sa ransomvér. V dôsledku toho sa nebude môcť tak ľahko šíriť v sieti ani v tom najhoršom prípade infekcie.

Cisco Security Services môže zabezpečiť okamžité roztriedenie v prípade reakcie na incident po jeho prepuknutí. Zefektívňujú aj zavádzanie AMP, NGFW a ďalších produktov riešení.

Hlavné funkcie

- Zabráni ransomvéru dostať sa do siete alebo jeho prevzatiu do notebookov
- Zabráni najhorším scenárom v súvislosti s ransomvérom v prípade, že sa dostane do siete

Služby zabezpečenia pomáhajú v boji proti ransomvéru

Tím spoločnosti Cisco poskytujúci bezpečnostné služby na riešenie incidentov môže v prípade prepuknutia ransomvéru poskytnúť služby pripravenosti na riešenie incidentov a reaktívnu reakciu na incidenty.

Navyše Cisco Security Integration Services (bezpečnostné integračné služby) riešia architektonické problémy na úrovni riešení. Zjednodušuje zavádzanie technológií riešení, ako sú AMP for Endpoints a Cisco Firepower NGFW. Náš tím disponuje hlbokými odbornými znalosťami v oblasti poskytovania integrovaných bezpečnostných riešení, ktoré urýchľujú prevzatie potrebných bezpečnostných technológií len s malým prerušením činnosti.

Všeobecnejšie povedané, organizácie musia zabezpečiť aj to, aby mali príslušnú technológiu na zálohovanie údajov a zavedené zásady na ochranu proti vplyvom napadnutia ransomvérom.

„Zabezpečili sme ochranu proti veľkému riziku internetového útočného vektora ransomvéru a výrazne sme zlepšili používateľské skúsenosti, pokiaľ ide o pripojenie k internetu.“

– Octapharma

Cisco Capital

Financovanie, ktoré vám pomôže dosiahnuť vaše ciele

Financovanie Cisco Capital® vám môže pomôcť získať technológiu, ktorú potrebujete na dosiahnutie svojich cieľov a udržanie si konkurencieschopnosti. Môžeme vám pomôcť znížiť kapitálové výdavky. Urýchlite svoj rast. Optimalizujte svoje investície a ich návratnosť. Financovanie Cisco Capital vám poskytne flexibilitu pri získavaní hardvéru, softvéru, služieb a doplnkového externého vybavenia. A je tu len jedna očakávaná platba. Služba Cisco Capital je k dispozícii vo viac ako 100 krajinách. Ďalšie informácie.

Výhody riešení Cisco

Ransomvér si cestu do vašej organizácie nájde pomocou akýchkoľvek potrebných prostriedkov. E-maily zamerané na neoprávnené získavanie údajov, napadnuté webové banery, nevyžiadané e-mailové správy – existuje mnoho vektorov, proti ktorým je potrebné sa chrániť. Len spoločnosť Cisco prináša bezpečnostnú architektúru, ktorá si poradí pri konfrontácii s problémom s ransomvérom. Samotné poukázanie na produkty nepostačuje. Naše riešenie je podporované špičkovým výskumom hrozieb realizovaným členmi tímu Talos, ktorí vykonali rozsiahly výskum ohrozenia ransomvérom a tým zvýšili účinnosť našej vrstvenej ochrany. Zablokujeme ransomvér a budeme s ním aj bojovať v prípade, že prekĺzne a dostane sa do vašej siete – čo sa ľahko môže stať nešťastnou realitou.

C22-737492-01 08/16