Cisco Ransomware Defense: Țineți la distanță amenințările de tip ransomware

Cum ar fi să nu vă mai îngrijorați în privința amenințărilor de tip ransomware, oricare ar fi metoda prin care încearcă să pătrundă? Numai Cisco vă poate oferi produsele și arhitectura de securitate adecvate în acest sens.

Prezentare generală

Fișierele și informațiile sunt esențiale pentru o organizație. Menținerea acestor informații și a productivității organizației dumneavoastră intacte și sigure nu este negociabilă.

Dar intervin amenințările de tip ransomware, software-ul rău intenționat sau malware-ul, care blochează informațiile din computerul unei persoane sau al unei organizații, cum ar fi documentele, fotografiile și muzica. Aceste fișiere nu vor fi eliberate până când utilizatorul nu plătește o taxă sau răscumpărare pentru deblocarea și recuperarea fișierelor. Fără protecția corespunzătoare, ransomware poate produce atât de multe daune unei companii, încât îi poate reduce activitatea la pix și hârtie.

Ransomware este, adesea, infiltrat prin intermediul kiturilor de vulnerabilitate, malvertising (reclame infectate pe un site web care conține malware), phishing (e-mailuri frauduloase, care par de încredere) sau campanii spam. Infectarea propriu-zisă poate începe în momentul în care cineva face clic pe un link sau pe un fișier atașat din e-mailurile de phishing. Infectările pot avea loc și atunci când utilizatorii navighează pe site-uri cu reclame rău intenționate, care infectează automat computerele.

Aici intervine Cisco® Ransomware Defense. Acesta reduce riscul de infectare cu ransomware printr-o abordare stratificată, de la DNS la terminal și la rețea, e-mail și web. Oferim protecție integrată printr-o abordare arhitecturală, care combină cea mai bună vizibilitate cu cele mai eficiente reacții împotriva atacurilor de tip ransomware.

Beneficii

- **Reduceți riscul de ransomware** astfel încât să vă puteți concentra pe desfășurarea activității.
- **Obțineți protecție imediată** cu soluții de securitate care pot bloca amenințările înainte să încerce să se înrădăcineze.
- **Obțineți vizibilitate și viteză de răspuns de neegalat** printr-o abordare arhitecturală de la nivelul DNS la rețea și la terminal.
- **Preveniți răspândirea în lateral a malware-ului** prin segmentarea puternică a rețelei.
- **Obțineți cercetările și informațiile Talos, lider în domeniul** combaterii ransomware.

O amenințare puternică, cu dezvoltare rapidă

Acesta este anul ransomware. Și se dovedește a fi foarte profitabil. Ransomware a devenit rapid cel mai profitabil tip de malware întâlnit vreodată.

FBI a declarat că este pe cale să devină o piață anuală de 1 miliard USD. Studiile Cisco Talos arată că o singură campanie de ransomware poate genera până la 60 milioane USD anual. Ransomware se bucură de atât de multă atenție încât a fost prezentat în emisiuni difuzate la televizor.

Atacatorii dispun de fondurile și dorința de a continua să inoveze în domeniul atacurilor de tip ransomware, care vor deveni mult mai agresive. Considerăm că ransomware va deveni capabil de autopropagare, cu scopul de a bloca numeroase rețele corporative. Acest lucru va readuce efectiv funcționalitatea infrastructurii IT la cea din anii '70.

Reacțiile curente în privința ransomware tind să evolueze în jurul produselor de tip single point. Trebuie să luăm în calcul o abordare arhitecturală care să facă față, având în vedere diversii vectori pe care îi vizează pentru a răspândi infectarea.

Această prezentare generală a soluției descrie diverși vectori și metode pe care le utilizează atacatorii. Protectorii trebuie să securizeze atât e-mailul, cât și internetul, să blocheze accesul la infrastructura rău intenționată de pe internet, să oprească toate fișierele ransomware care își croiesc drum către un terminal, să blocheze orice apel invers de comandă și control utilizat și să prevină mișcarea laterală simplă a atacurilor ransomware în cazul în care apare o infecție.

Ce cumpărați

Cisco Ransomware Defense reunește toate soluțiile necesare ale arhitecturii de securitate Cisco pentru a depăși provocarea ransomware. Puteți alege toate soluțiile sau le puteți selecta pe cele care îndeplinesc nevoile de securitate imediate.

Ransomware Defense conține:

- „Cisco Umbrella”, care blochează amenințările la nivel DNS, departe de rețeaua dumneavoastră.
- „Cisco Advanced Malware Protection (AMP)” pentru terminale, care blochează fișierele ransomware rău intenționate să ruleze în terminale.
- „Cisco Email Security”, atât în cloud, cât și local, care oprește mesajele de phishing și spam care au intenția de a introduce ransomware.

- „Advanced Malware Protection” poate fi adăugat imediat la produsele de securitate pentru e-mail printr-o licență simplă pentru analiză statică și dinamică (mediu de testare) a fișierelor atașate necunoscute, care trec prin gateway-ul Cisco pentru securitatea e-mailurilor.
- „Cisco Firepower™”, un firewall de generație nouă (NGFW), care blochează traficul de comandă și control și orice fișier rău intenționat care traversează rețeaua.
- „Cisco ISE” prin rețeaua Cisco segmentează rețeaua unei companii în mod dinamic, astfel încât atacurile ransomware să nu se poată răspândi în lateral.

Grație Ransomware Defense, organizațiile pot utiliza rețeaua ca pe un mijloc de a opri răspândirea atacurilor ransomware. În cel mai rău caz al unei infecții, acestea nu se vor mai putea propaga la fel de ușor în rețea.

Serviciile Cisco Security pot oferi o triere imediată în cazul reacțiilor în urma unui incident cauzat de o infecție. Acestea fluidizează implementarea AMP, NGFW și a altor soluții.

Capabilități principale

- Blocați pătrunderea atacurilor ransomware în rețea sau descărcarea acestora în laptopuri.
- Opriți atacurile ransomware în cele mai grave situații, cele în care acestea pătrund în rețea.

Serviciile Cisco Security ajută la combaterea atacurilor ransomware

În caz de incidente, echipa Cisco Security Services poate oferi atât răspuns activ, cât și răspuns reactiv la incidente, în cazul atacurilor ransomware.

În plus, Cisco Security Integration Services ajută la depășirea provocărilor arhitecturale de la nivelul soluțiilor. Aceste servicii fluidizează implementarea tehnologiilor de soluții, cum ar fi AMP pentru terminale și Cisco Firepower NGFW. Echipa noastră are o experiență vastă în furnizarea de soluții de securitate integrate pentru a grăbi adoptarea tehnologiilor de securitate necesare, cu foarte puține întreruperi.

Organizațiile trebuie să se asigure că dețin tehnologiile și politicile corespunzătoare pentru backupul datelor, în vederea reducerii impactului unei infectări cu ransomware.

„Am acoperit un risc uriaș în vectorul atacurilor web ransomware și am îmbunătățit semnificativ experiențele utilizatorilor cu privire la conectivitatea la internet.”

– Octapharma

Cisco Capital

Finanțare care vă poate ajuta să vă atingeți obiectivele

Finanțarea Cisco Capital® vă poate ajuta să obțineți tehnologia de care aveți nevoie pentru a vă atinge obiectivele și pentru a rămâne competitiv. Vă putem ajuta să reduceți cheltuielile de tip CapEx. Accelerați-vă dezvoltarea. Optimizați-vă rentabilitatea investiției. Finanțarea Cisco Capital vă oferă flexibilitatea de a achiziționa hardware, software, servicii și echipamente suplimentare de la o terță parte. Și există o singură plată previzibilă. Cisco Capital este disponibil în peste 100 de țări. Aflați mai multe.

Avantajul Cisco

Atacurile de tip ransomware vor găsi o cale de a pătrunde în organizația dumneavoastră prin orice metodă. E-mailuri de phishing, bannere web compromise, spam: mulți vectori trebuie să fie protejați. Numai Cisco poate oferi o arhitectură de securitate care face față provocărilor privind atacurile ransomware. Doar produsele punctuale nu vor fi suficiente. Soluția noastră este susținută de Grupul de cercetare Talos lider în domeniu, care ne-a ajutat în desfășurarea cercetării detaliate a atacurilor ransomware, participând la furnizarea protecției noastre eficiente stratificate. Vom bloca atacurile ransomware și inclusiv vom lupta împotriva acestora în cazul în care pătrund în rețeaua dumneavoastră, situație care poate fi cât se poate de reală.

C22-737492-01 08/16