STÄNG UTE RANSOMWARE INNAN DET SPRIDS

En automatiserad lösning för att stoppa ett utbrott av ransomware inom din organisation

Låt oss inse fakta: Även de mest välskyddade organisationerna faller offer för ransomware. Cyberbrottslingar utvecklar ständigt nya och innovativa sätt att besegra traditionella, upptäcktsmetoder baserade på förebyggande insats. För att skydda sig från ransomware måste en organisation utveckla sina säkerhetsförsvar och införa ett lagerbaserat tillvägagångssätt. När ransomware utlöser sin last (kryptering) kan det vara för sent för befintlig säkerhet att reagera. Vid det här laget är det viktiga hur snabbt du kan stoppa den olagliga krypteringen av upp till 10 000 filer per minut.

Ett lagerbaserat tillvägagångssätt inkluderar en kompletterande lösning för att upptäcka och stoppa illegitim kryptering när den pågår. Det kan göra det genom att övervaka filaktiviteten på fil- och molnresurser. Så snart lösningen identifierar pågående kriminell kryptering och filkorruption, reagerar den och isolerar användaren som orsakar det.

Vi introducerar Ricohs lösning för ransomware-inneslutning-RICOH RansomCare drivs av BullWall - ett unikt och beprövat försvarslager. Över 20 detekteringssensorer utvärderar varje filändring på övervakade delningar. Om kontrollteckнen på ransomware (illegitim kryptering) initieras, och filer aktivt krypteras på övervakade fil- och molnresurser, reagerar RICOH RansomCare genom att isolera den komprometterade enheten och användaren för att stoppa den kriminella krypteringsprocessen. Lösningen är en viktig del av din övergripande försvarsstrategi, och ger kritiskt säkerhetsskydd för en liten del av din tillgängliga säkerhetsbudget.

Kan du svara på dessa frågor i händelse av ett utbrott av ransomware?

- Hur ser du vilka filer som är krypterade och var de finns?
- Hur identifierar du vilken användare och vilken enhet som krypterar filer?
- Hur stoppas den pågående krypteringen snabbt innan betydande skada uppstår?
- Hur lång tid tar det för dig att återställa hundratusentals filer, och vad är den totala kostnaden för stillestånd?
- Hur lång tid behövs för att korrekt rapportera till datamyndigheter om tusentals filer med personlig information har krypterats olagligt?

RICOH
imagine. change.

Varför ransomware är viktigt

Nu mer än någonsin har C-sviten (t.ex. CIO, CISO, CFO och CEO) en betydande andel i att säkra data och intellektuellt kapital för att skydda personligt identifierbar information (PII), intäkter, upprätthålla kundlojalitet och säkra aktieägarvärde. Traditionella säkerhetsförsvar fokuserar på att förhindra skadlig programvara från att exekvera, om slutpunkter är målet för skadlig programvara. Men vad händer om de misslyckas? Ransomware är en annan historia. Det har förlamat organisationer trots att de har de bästa säkerhetslösningarna på plats. Organisationer i dag bör överväga driftsätta ytterligare en försvarslinje för att fungera som ett "sprinklersystem" om förebyggande säkerhetslösningar skulle misslyckas.

Det är avgörande att organisationer inte enbart förlitar sig på ett reaktivt svar på moderna skadliga hot. Vi hör dagligen rapporter om hur denna strategi har visat sig misslyckas. Framtidens försvarsstrategi måste innefatta affärskontinuitet och katastrofåterställning, för att möjliggöra automatiska varningar, ett avstängningssvar och snabb återhämtning utan de enorma kostnader som ofta är förknippade med ransomwareattacker.

Hur det fungerar

Med en snabbt växande attackyta för att försvara och flera ingångspunkter för skadlig programvara till organisationer idag, levererar RICOH RansomCare ett 24/7 automatiskt inneslutningssvar på utbrott av ransomware med inbyggd respons och rapportering. Det spelar ingen roll vilken användare eller vilken enhet som utlöste krypteringen. Det spelar heller ingen roll om attacken är en känd eller okänd variant av ransomware eller om utbrottet startade på en slutnod, en mobiltelefon, en IoT-enhet, via e-post, USB eller distribuerades av någon inom din organisation. RICOH RansomCare undersöker heuristiken för varje fil som nås av en användare på övervakade filresurser, antingen på plats eller i molnet, utan att orsaka några nätverkskostnader. När RICOH RansomCare upptäcker pågående kryptering och filkorruption på övervakade delningar, utlöses en varning omedelbart och ett svar utlöses för att inaktivera och isolera enheten och användaren som krypterar dina data.

RICOH RansomCare fungerar också i virtuella miljöer som Citrix-servrar/sessioner, terminalservrar/sessioner, Hyper-V, VMware och molnet, inklusive Azure och Amazon AWS/EC2, SharePoint, Google Drive och Microsoft 365. Ett brett utbud av anpassningsbara isoleringsmetoder kan användas, såsom tvingad avstängning, inaktivera VPN, inaktivera AD-användare, inaktivera nätverksåtkomst, återkalla molnbehörigheter och många andra. Integrering genom RESTful API med andra säkerhetslösningar innebär att dina säkerhetsteam kan förena säkerhetshantering över ett allt mer komplext hav av slutpunkter.

Problemfri fjärr-Installation

RICOH RansomCare är en lösning utan krav på personalnärvaro och är inte installerad på slutnoder, befintliga servrar eller filservrar. Den påverkar inte nätverksprestandan. Filbeteendeövervakning utan krav på personalnärvaro och maskininlärningstekniker driftsätts med lätthet på fyra till sex timmar, och RICOH RansomCare kommer att konfigureras efter din miljö. RICOH RansomCare har Cloud Connectors för organisationer som använder Microsoft O365 (SharePoint, Teams, OneDrive) och Google Drive. Full integration med andra säkerhetslösningar som Cisco ISE och Windows Defender ATP eller SIEM-system är tillgängligt via RESTful API, vilket gör att dina säkerhetsteam kan förena säkerhetshanteringen över ett allt mer komplext hav av slutnoder.

- Ingen molninstallation
- Ingen slutnodsinstallation (utan krav på personalnärvaro)
- Ingen filserver/lagringsinstallation

Varningar och integrationer

RICOH RansomCares inbyggda varningstjänster

E-postaviseringar
SMS-larm
Mobil ”SOC”
API till andra system

2-vägsgränssnitt till Restful

Splunk
Cisco ISE
Windows Defender
Aruba
IBM Radar
McAfee
Symantec
TrendMicro
ForeScout
och många fler

Ransomware utvärderingstest

Vi kan utföra ett utvärderingstest för ransomware där en säker och kontrollerad simulator av ransomware används för att simulera nolldagars filkryptering och snabba filbyten. Vi kommer sedan att testa RICOH RansomCare i din miljö för att visa hur lösningen reagerar på ett utbrott av filkryptering. Fråga en säljare för mer information.

RICOH
imagine. change.