Truffe del CEO, phishing, ransomware: un livello di sicurezza robusto con Advanced Threat Protection

La sfida

Al giorno d'oggi, la maggior parte della posta elettronica è costituita da messaggi indesiderati. Oltre all'enorme quantità di spam e virus abituali, le aziende e i dipendenti si trovano sempre più spesso ad affrontare minacce complesse, come gli attacchi di ingegneria sociale e phishing. Spesso, i meccanismi di sicurezza tradizionali non sono più in grado di fornire una protezione sufficiente contro queste e-mail personalizzate. Il malware, inoltre, viene modificato a intervalli sempre più brevi e circola costantemente in nuove varianti.

Il background

Quando appaiono per la prima volta, le nuove minacce sono per natura sconosciute agli scanner di virus. Poiché non sono ancora disponibili firme corrispondenti, le e-mail infette si diffondono in un tempo molto breve. A questa dinamica si aggiunge il fatto che i criminali informatici impiegano mezzi di attacco sempre più sofisticati con i quali cercano di impossessarsi di informazioni sensibili. Le soluzioni di sicurezza convenzionali hanno difficoltà a distinguere tra queste e-mail e i messaggi legittimi. Gli attacchi riusciti non solo portano a perdite di dati con gravi conseguenze o al fallimento dei sistemi, ma anche a costi enormi e danni alla reputazione. Ecco perché è fondamentale che le aziende adattino le loro politiche di sicurezza alla realtà attuale.

La soluzione

Il livello di protezione di base fornito da Essential Protection di Retarus Email Security utilizza già misure di salvaguardia complete e fino a quattro diversi scanner di virus, consentendo di filtrare in modo affidabile la stragrande maggioranza delle e-mail pericolose. Con il livello di protezione avanzato offerto da Advanced Threat Protection, le aziende possono ora utilizzare una vasta gamma di funzioni aggiuntive per proteggersi dalle minacce diverse dalle classiche e-mail di virus e spam.

Vantaggi per i clienti

- Protegge le comunicazioni aziendali sensibili
- Sicurezza IT pronta per il futuro
- Evita le perdite finanziarie dovute alle frodi
- Educa il personale sui rischi del phishing e sugli altri rischi
- Fornisce protezione dai danni alla reputazione dovuti alla perdita di dati

I vantaggi in breve

- Identificazione affidabile di nuove varianti di malware e virus
- Protezione avanzata contro l'ingegneria sociale
- Analisi per mezzo di fonti di dati altamente specializzate e algoritmi proprietari
- Report e analisi dettagliati
- Integrazione perfetta con altri servizi e-mail della piattaforma Retarus

Caso d'uso

I criminali informatici utilizzano sempre più spesso l'ingegneria sociale per lanciare attacchi che comportano il rischio di danni finanziari per le aziende. Nelle truffe del CEO, ad esempio, i criminali informatici si spacciano per l'amministratore delegato dell'azienda e utilizzano e-mail fasulle per istruire le loro vittime a trasferire grandi somme di denaro. Retarus CxO Fraud Detection permette di riconoscere i falsi indirizzi mittenti utilizzati per questi attacchi mirati e di avvisare il personale della presenza di e-mail fraudolente. Questo risultato viene ottenuto tramite un'analisi avanzata dell'intestazione delle e-mail e per mezzo di algoritmi specializzati, che identificano in modo affidabile lo spoofing dell'intestatario o lo spoofing del dominio.

Inoltre, Retarus Time-of-Click Protection facilita la prevenzione degli attacchi di phishing e la conseguente perdita di dati sensibili. La tecnologia controlla inoltre tutti i link contenuti nelle e-mail per gli indirizzi di destinazione per i quali si sospetta un'azione di phishing. Se nuove informazioni raccolte nel tempo mostrano che la destinazione può essere pericolosa, il link viene bloccato e all'utente viene invece mostrato un avviso di sicurezza.

Per proteggere meglio le aziende dal malware in continua evoluzione, come il ransomware, nell'ambito della Advanced Threat Protection, Retarus offre anche Deferred Delivery Scan e analisi approfondite di tipo Sandboxing. Deferred Delivery Scan effettua una seconda scansione ritardata di determinati allegati. A tal fine, l'e-mail viene trattenuta per alcuni minuti prima di essere consegnata al destinatario. In caso di attacchi che utilizzano un malware nuovo, questo ritardo consente di utilizzare eventuali firme dei virus aggiornate, che non erano disponibili al momento della prima scansione. Con la soluzione Sandboxing, anch'essa offerta nel contesto di Advanced Threat Protection, prima di essere consegnati ai destinatari, gli allegati vengono eseguiti in un ambiente di test virtuale e sicuro ed esaminati al fine di rilevare eventuali comportamenti irregolari attraverso complesse procedure di simulazione.

Lo sapevate che…

Ogni giorno, in tutto il mondo vengono registrati più di 390.000 nuovi casi di malware. Questo significa che in media vengono rilasciate circa 270 nuove varianti di virus al minuto.

Altri scenari

Postdelivery Protection
L'innovativa tecnologia di Retarus Patient Zero Detection® identifica inoltre le e-mail dannose già recapitate. In caso di sospetto, gli amministratori vengono immediatamente informati, in modo da evitare ulteriori danni.

Crittografia Sicura
I dati sensibili non devono cadere nelle mani sbagliate. Con Retarus Email Encryption le aziende possono garantire la riservatezza delle loro comunicazioni e rispettare senza difficoltà le normative su protezione e riservatezza dei dati.

Email Live Search
Con Email Live Search integrato in Retarus Essential Protection, Retarus offre un servizio di analisi rapida ed efficiente del recapito delle e-mail. Alcuni dipendenti di supporto presso l'azienda del cliente sono in grado di tracciare in dettaglio quali filtri di sicurezza sono stati applicati per ogni specifico messaggio e individuare il momento in cui un'e-mail è passata attraverso i diversi punti dell'infrastruttura.