Scheda Tecnica

Servizio Email security

1. Descrizione generale

Il servizio di Advanced Email Security consente di filtrare tutte le e-mail interne e il traffico e-mail in entrata per proteggere le aziende dalle minacce trasmesse via e-mail e dalle fughe di dati. Offre sia il filtraggio dello spam che la protezione contro le minacce avanzate come il phishing, lo spam, la compromissione delle e-mail aziendali e l'acquisizione di account.

Utilizziamo le nostre tecnologie di sandboxing per analizzare tutti i link e i documenti. URLsand e QuickSand analizzano rapidamente tutti i link e i documenti alla ricerca di codice attivo e comportamenti evasivi. Questo impedisce agli utenti di visitare link pericolosi o di ricevere e aprire file dannosi.

2. *Descrizione prodotto e funzionalità*

Il servizio di eMail Security è basato sul prodotto LibraEsva.

Non è solo un classico antiSpam, ma un vero e proprio strumento di protezione su molteplici livelli.

Il servizio offre ben 14 Livelli di filtraggio sia in Inbound che in Outbound, in particolare:

- Reputation: RBL Pubbliche, proprietarie,
- Attendibilità: SPF, DNS, DKIM , DMARC
- Machine learning: Filtro Bayesiano , Semantica
- Sicurezza: Antivirus, Sandboxing, Image analysis
- Sociali: Advanced Trust Engine

Il motore di URLSAND Sandbox consente un approccio proattivo di protezione da attacchi tramite link:

- Riscrittura dei link
- Posticipo dell'analisi al click dell'utente
- Analisi in tempo reale dei link presenti nelle e-mail da qualsiasi dispositivo

Il motore di QUICKSAND Sandbox abilita funzionalità di DEEP DISCOVERY AND DISARM dei contenuti attivi negli allegati MS Office, PDF ed RTF:

- Ricerca di Macro e Contenuti attivi
- Categorizzazione - sicuri - pericolosi - sospetti - criptati
- Disarmo contenuti pericolosi o indeterminati

Per il servizio di eMail Security verrà operata la configurazione congiuntamente tra il referente del cliente e il consulente di SOC CD.

2.1 Adaptive Threat Engine

La funzionalità di Adaptive Trust Engine (A.T.E.) consente un tracciamento dinamico delle relazioni tra mittenti e destinatari delle e-mail; tutte le transazioni sono tracciate e monitorate per misurare il “TRUST” e osservare chi comunica abitualmente all'interno della vostra organizzazione.

Adaptive Trust Engine utilizza l'apprendimento automatico e l'intelligenza artificiale insieme all'analisi dei dati storici per apprendere in modo rapido e automatico i modelli di comunicazione legittimi specifici per ogni mittente e destinatario, rendendo più semplice l'individuazione delle e-mail anomale.

2.2 Rilevamento di mittenti insoliti

Sfruttando le informazioni dell'AdaptiveTrustEngine, siamo in grado di intervenire solo quando è necessario.

Il nostro rilevamento del FirstTimeSender interviene solo quando qualcuno non ha alcun rapporto con voi o con la vostra organizzazione.

Le relazioni con i partner sono complesse da gestire, per cui, utilizzando algoritmo di intelligenza artificiale, prendiamo in considerazione informazioni quali la quantità di contatti storici con l'organizzazione e gli utenti, il contenuto dell'e-mail e altro ancora per determinare i mittenti che inviano per la prima volta e se è necessario aggiungere un messaggio.

2.3 Protezione da Attack Takeover (ATO)

Il servizio di Advanced eMail Security fornisce monitoraggio e intelligence in tempo reale per mitigare le frodi umane e automatiche prima che abbiano un impatto sull'azienda, senza interrompere l'esperienza del cliente.

Grazie a funzionalità dedicate basate sulla nostra tecnologia proprietaria Adaptive Trust Engine AI, Libraesva ESG è in una posizione unica per bloccare le ATO con una difesa che si adatta ai cambiamenti nei modelli di attacco e alle riorganizzazioni, in quanto esamina la cronologia e i modelli di comunicazione, trasferendo il valore della relazione umana nella comunicazione digitale.

Sfruttando le informazioni basate sull'Adaptive Trust Engine Ai, siamo in grado di identificare le attività insolite della casella di posta elettronica, come l'invio massiccio di messaggi a contatti esistenti o a destinatari completamente nuovi, tenendo in sospeso i messaggi sospetti e inviando una notifica all'utente.

2.4 Sanitizzazione dei documenti

La sanificazione comporta la pulizia o l'eliminazione nei file dal contenuto attivo nascosto pericoloso (ad esempio, malware, macro, javascript, ecc.). Un esempio di codice dannoso potrebbe essere uno script invisibile e dannoso incorporato in un documento. Per rimediare a questo problema è necessaria una sanificazione strutturale per proteggere l'organizzazione da potenziali danni.

I documenti con contenuto attivo incorporato esistono ovunque. Il suo scopo è fornire all'utente un'esperienza più interattiva. I cyber-terroristi, tuttavia, inseriscono i propri contenuti attivi in documenti creati ad hoc o compromessi, ad esempio in documenti *MS Office o PDF* distribuiti come allegati.

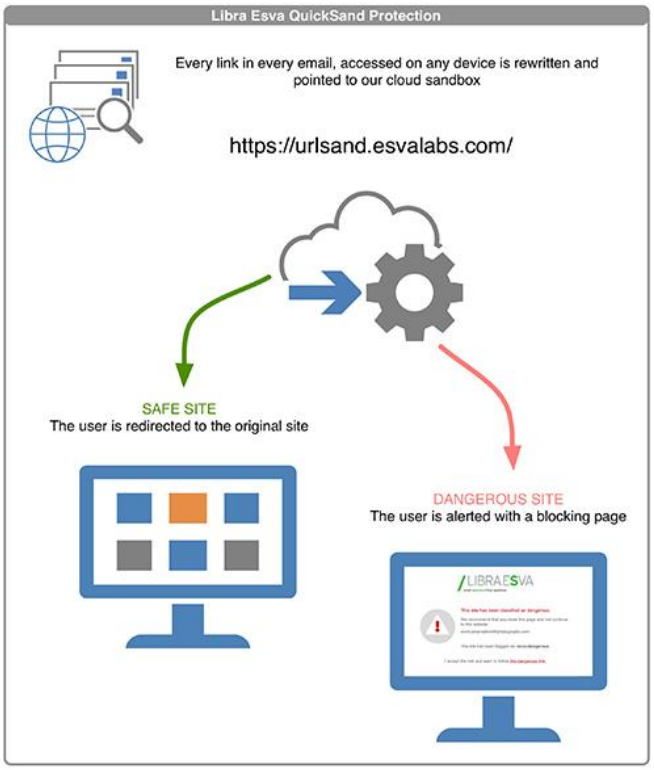
Il servizio offerto è in grado di rilevare e classificare i contenuti attivi in tutti i documenti Microsoft Office, RTF e PDF. In base ai risultati dell'analisi, si può scegliere se rimuovere il contenuto attivo e consegnare il documento sanificato o bloccare l'intero documento.

2.5 Protezione dei link (URL) al momento del "clic"

Come parte del nostro servizio, la difesa UrlSand di Libraesva blocca attivamente gli URL dannosi delle e-mail per proteggere da attacchi di spear-phishing, exploit zero-day e ransomware.

Ogni URL, non solo quelli non catalogati, in ogni e-mail, è protetto. Su ogni dispositivo. Estendete la protezione dei link quando vi si accede, non solo quando arriva l'e-mail.

La nostra sandbox URLSand non è solo un controllo aggiuntivo della blacklist al momento del clic, ma una scansione completa delle pagine, che rileva eventuali malware annidati e pagine sospette, esaminando il contenuto offuscato e seguendo tutti i reindirizzamenti.

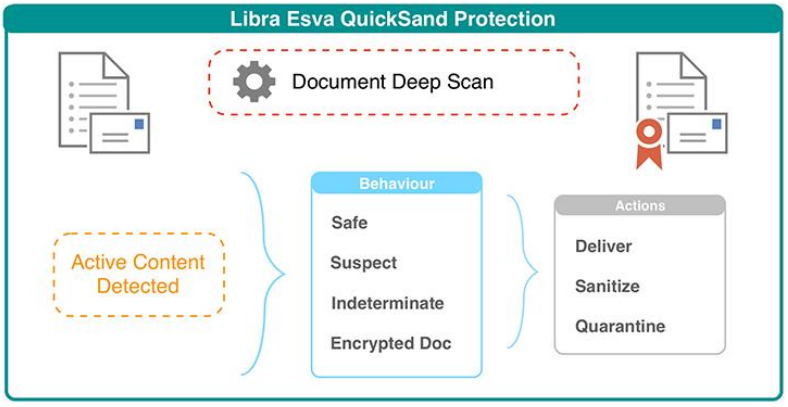


2.6 Difesa dalle minacce avanzate in documenti "armati"

Come parte del servizio di Advanced eMail Security, vengono utilizzate tecniche sofisticate per valutare le minacce avanzate che vengono tradizionalmente ignorate dalle soluzioni basate sulle firme e sulla reputazione.

La funzionalità di sandboxing delle minacce zero-day avviene interamente nel gateway, senza rivelare alcun documento a nessuno.

In questo processo non sono coinvolti ambienti di sandboxing nel cloud, ma i vostri dati vengono conservati al gateway.



3. *Descrizione Servizio Gestito di eMail Security*

Il prodotto LibraEsva, scelto per le sue caratteristiche, è un abilitante del servizio che viene erogato al cliente.

Il servizio consente al cliente di avere un pool di esperti che:

- Effettuano un tuning continuo della Piattaforma
- Aggiornano continuamente le regole di whitelisting e blacklisting a seguito di segnalazioni degli utenti finali
- A seguito di richieste di sblocco mail da parte degli utenti finali, effettuano verifiche puntuali per avere la certezza che non siano mail malevole (oltre alle verifiche automatiche della piattaforma)
- Effettuano attività di Threat Hunting sul perimetro monitorato
- Realizzano reportistica per il cliente finale, inserita nei report trimestrali di servizio