LIBRAESVA
EMAIL SECURITY

Email Security Tester vademecum

L'Email Security Tester Libraesva ti consente di verificare facilmente il livello di sicurezza della tua azienda rispetto alle varie minacce veicolate tramite email.

Grazie a questa guida potrai interpretare velocemente e autonomamente i risultati del test, identificando eventuali aree di criticità della soluzione di email security che stai utilizzando.

Come funziona?

Tutto molto semplice! Basta cliccare questo **LINK**, inserire un indirizzo email del dominio che si vuole verificare e del quale si ha l'accesso, proseguendo poi con l'inoltro della richiesta.
All'indirizzo indicato, verrà recapitata un'email con la quale si chiede conferma per proseguire con il test. Una volta confermato, il test avrà inizio e verranno inviate 15 email oggetto d'analisi, contenenti minacce GIA' NOTE che qualsiasi sistema di email security, correttamente istallato, dovrebbe riconoscere e bloccare.

1. **Spoofed envelope sender**
2. **HTML analysis**
3. **Executable file**
4. **Virus attachment**
5. **Outlook Conditional Comment**
6. **Malware URI**
7. **Zero Width Spaces link**
8. **Base HTML Tag link**
9. **HTML JS Redirect Attachment**
10. **RFC-Abused HTML Attachment**
11. **Active PDF**
12. **PDF with malicious text link**
13. **PDF with malicious link**
14. **ZIP Archive with JS**
15. **MS Word Document with external contents**
16. **Business Email Compromise**

Il servizio è pensato per essere completamente svincolato dall'adozione dell'Email Security Gateway Libraesva.
Quindi, è possibile utilizzare questo servizio anche su un differente email security gateway.
Se invece utilizzi la soluzione Libraesva, accertati di averla configurata correttamente, altrimenti le email del test potrebbero non essere riconosciute come pericolose e, di conseguenza, non venire bloccate.
Spesso i nostri partner, al termine dell'installazione e configurazione di ESG, usano questo servizio per testarne il corretto funzionamento.

Westcon

1. Spoofed envelope sender

Questo test prevede che una email venga spedita con l'indirizzo someone@dominioazienda.
Libraesva Email Security Gateway non è ovviamente autorizzato ad inviare email per conto di questo dominio.

✓ La vostra soluzione di email security dovrebbe **RIFIUTARE** messaggi di questo tipo. Se avete ricevuto questa email, siete vulnerabili di fronte ad attacchi di phishing.

2. HTML analysis

Questa email ha lo scopo di verificare se l'antispam riconosce le minacce presenti all'interno del contenuto del messaggio.
Alcuni TAG HTML sono considerati potenzialmente pericolosi, perchè possono causare l'installazione di Malware e Ramsonware.

Javascript

Se non correttamente disabilitati all'apertura, vedrete comparire un popup sulla mail.

Phishing link

Il seguente link è presentato come libraesva.com ma se il l'hyperlink non è stato correttamente bloccato, punterà ad una pagina diversa www.example.com.

✓ La tua soluzione di email security **DEVE** rinterrompere il collegamento o sottolinearne da discrepanza.
www.libraesva.com

Iframe

✓ Se non correttamente disarmato , vedrai una pagina di example.

3. Executable file

Nella mail ricevuta vi è un allegato nela quale è presente un file eseguibile chiamato putty.exe
Si tratta di un'applicazione nota, che da sola non fa alcuna azione malevola.
Può essere però utilizzata, se modificata, per eseguire del codice malevolo, inviandolo in modalità remota al tuo sistema.

✓ La tua soluzione di email security **DEVE** rimuovere questo tipo di allegato

4. Virus attachment

In allegato alla mail ricevuta, troverete un FINTO esempio di Virus usato per testare il livello di protezione degli antivirus.
Questo è un codice conosciuto da tutti gli antivirus ed è utilizzato di proposito per testare le funzionalità e i tempi di reazione di antivirus basati su Firma.

✓ La tua soluzione di email security **DEVE** rimuovere questo tipo di file; in seguito dovresti ricevere un messaggio di report che lo evidenza come " EICAR TEST VIRUS – DETECTED"

5. Outlook Conditional Comment

Questa email ha lo scopo di verificare se la soluzione di email security in uso riconosce le minacce che fruttano le Outlook Conditional Comments.
Microsoft Outlook for Windows usa commenti in HTML per nascondere al loro interno link malevoli o commenti che vengono tendenzialmente ignorati dai client email ma che possono divenire veicoli di attacco a macchine windows.

Approfondimento sul nostro BLOG.

[Conditional Comment]

Se non state usando Microsoft Outlook for Windows o se il vostro Email Security Gateway è in grado di disarmare l'HTML, questa mail è sicura ed il test finisce qui.

Se, invece, stai leggendo questo testo, vuol dire che **i commenti NON sono stati disarmati**. Stai usando Microsoft Outlook for Windows: fai attenzione, i commenti sono veramente pericolosi!]

Il link di seguito è un malware (innocuo) che testa le URI nascoste dietro le sicure URL. La tua soluzione di email security **DEVE** proteggerti o **RIMUOVERE** questo link.

Link potenzialmente dannoso

6. Malware URL

Questa email testa l'abilità della soluzione di email security di riconoscere una URL malevola in tempo reale, così che uno 0-day o 0-hour venga bloccato appena scoperto.

Il link riportato qui sotto è sicuro nella sua veste grafica ma la URI a cui fa riferimento punta ad un malware test (sicuro e conosciuto). L'email non può essere solitamente bloccata dal gateway per la presenza di una URI diversa dal link.

✓ La tua soluzione di email security **DEVE** intercettare la minaccia e **CONTROLLARE** al momento del clic, tramite un sistema di sandboxing degli allegati.

Qui il link

7. Zero Width Spaces link

Questa email verifica la capacità della soluzione di email security di riconoscere e bloccare link Zero Width Spaces, usati solitamente per bypassare i controlli di sicurezza.
Un link di questo tipo, può bypassare i controlli ed essere così consegnato all'utente.

✓ Se il link non è stato riscritto o disarmato, cliccando su di esso arriverai alla pagina Malware di Google, utilizzata come test.

8. Base HTML Tag link

Questa email ha lo scopo di valutare l'abilità della soluzione di email security di riconoscere e bloccare una vulnerabilità conosciuta come baseStriker, che permette di mandare email malevole che bypassano i controlli di sicurezza.

Un link scritto con un URL Base può bypassare le soluzioni di sicurezza ed essere consegnato, senza protezione, alla casella dell'utente.

✓ Se il link non è stato riscritto o disarmato, cliccando su di esso arriverai alla pagina Malware di Google, utilizzata come test.

9. HTML JS Redirect Attachment

In allegato a questa email è presente un file HTML che rimanda ad una pagina pericolosa.

✓ La tua soluzione di semail security **DEVE** rimuovere questo allegato o **BLOCCARE** l'intera email.

10. RFC-Abused HTML Attachment

In allegato a questa email è presente un file HTML slavato come “application/html”. La dicitura “application” fa riferimento a un file generico che, per tale, motivo viene spesso lasciato passare dai controlli del gateway.

✓ La tua soluzione di semail security **DEVE** rimuovere questo allegato o **BLOCCARE** l’intera email.

11. Active PDF

Nell’email ricevuta è allegato un PDF con contenuto attivo.
Il contenuto attivo è, potenzialmente, un file eseguibile che, a seguito delll’apertura, si installa sul computer. Potrebbe essere anche un ransomware.

✓ La tua soluzione di email security **DEVE** disarmare questo contenuto attivo o **RIMUOVERE** l’intero file disarlmarlo non è possibile.

12. PDF with malicious text link

In allegato a questa email, è presente un tipico PDF con un link testuale. Di solito questi link puntano a pagine malevole. Questo è un esempio ed è, quindi, assolutamente inerme; il suo scopo è dimostrare come il “plain text” in forma di link può rimandare ad un sito pericoloso.

✓ La vostra soluzione di email security **DEVE BLOCCARE** l’allegato o **RIMUOVERE** il Link

13. PDF with malicious link

In allegato a questa email è presente un tipico PDF con un link inserito nel documento stesso. Questo è un esempio ed è, quindi, assolutamente inerme; olo scopo è dimostrare che i link “embedded” in forma di link possono rimandare ad un sito pericoloso.

✓ La tua soluzione di email security **DEVE** rimuovere questo link dal “View Now” dell’immagine, disarmare il documento o prevenire la possibilità che l’utente possa cliccare su questo link.

14. ZIP Archive with JS

In allegato è presente un archivio Compresso che contiene un file eseguibile.

✓ La tua soluzione di email security **DEVE** rimuovere il contenuto attivo o l’intero file, se impossibilitato a rimuovere solo la parte pericolosa.

15. MS Word Document with external contents

Utilizzare i documenti di Microsoft per inviare un payload è una pratica vecchia quanto i documenti stessi e nell’arco degli anni si sono visti nascere nuovi e sempre più sofisticati vettori di attacco.

Questo inerme esempio consente di scaricare uno script eseguibile, contenente un comando di PowerShell all’apertura del documento.

✓ La tua soluzione di email security **DEVE** rimuovere il contenuto attivo o l’intero file, se impossibilitato a rimuovere solo la parte pericolosa.

15. MS Word Document with external contents

Utilizzare i documenti di Microsoft per inviare un payload è una pratica vecchia quanto i documenti stessi e nell'arco degli anni si sono visti nascere nuovi e sempre più sofisticati vettori di attacco.

Questo inerme esempio consente di scaricare uno script eseguibile, contenente un comando di PowerShell all'apertura del documento.

✓ La tua soluzione di email security **DEVE** rimuovere il contenuto attivo o l'intero file, se impossibilitato a rimuovere solo la parte pericolosa.

16. Business Email Compromise

Con il termine Business Email Compromise (o Whaling) si fa riferimento a un attacco phishing con il quale l'attaccante impersonifica un "C-Level", con l'intento di trarre in inganno la propria vittima e costringerla a fare un trasferimento di denaro o condividere informazioni sensibili. Il mittente viene visualizzato in questa mail è "l'indirizzo selezionato nel test" ma il destinatario di un eventuale replay è qualcun altro quindi

✓ La tua soluzione di email security **DEVE** notificare questa email come tentativo di Whaling.

Approfondimento sul nostro BLOG.

Per gli utenti Libraesva ESG
Se questa pagina non è stata notificata come tentativo di whaling, si può accedere alla pagina System Content Analysis Whaling & Phishing Highlight e aggiungere l'indirizzo e la persona sotto i possibili utenti impersonificati.

Westcon /LIBRAESVA

CONTATTACI PER MAGGIORI INFORMAZIONI:

@: Elisa.Santariello@Westcon.com
m: +39 345.1650790
w: https://www.westconcomstor.com/it/it.html