L’Email è strumento business e veicolo di contagio

DIGIWAY

Introduzione

Con il nostro partner Libraesva, leader italiano della mail security, abbiamo realizzato una serie di brevi articoli che pubblicheremo su Linkedin, sul tema della gestione sicura e conforme alla normativa delle email aziendali. Lo scopo sarà aumentare la conoscenza dei rischi più comuni, aumentare la consapevolezza degli utenti per ridurre o eliminare i comportamenti a rischio e valutare la conformità normativa della gestione delle email.

CAPITOLO UNO

Email: elemento essenziale dei processi business critical digitali ma anche porta d'ingresso preferita dai cybercriminali

La posta elettronica si è conquistata, nel corso degli ultimi 40 anni, un posto di primo piano nelle comunicazioni aziendali ed interaziendali. La casella postale di ciascuno di noi è anche il repository consueto di molte informazioni.

Ciò è accaduto per due ragioni, essenzialmente:

- grande facilità d'uso
- capacitò di collaborare tra aziende senza istituire strumenti ad hoc

Spesso essa svolge, infatti, il compito di nastro trasportatore di allegati e per questo compito si presenta al suo utente come "facile e comoda" due elementi che sono spesso in antitesi con la sicurezza.

Questo ruolo, è assolutamente centrale nella tavolozza delle comunicazioni soprattutto con altre aziende, in particolar modo delle PMI, che ben difficilmente ricorrono a soluzioni differenti.

È proprio questa ubiquità della posta elettronica e questa affezione, quasi monomaniaca, alla posta stessa a creare delle grandi opportunità al cybercrime ed a rendere complesso il problema della protezione della posta elettronica stessa.

Per le aziende, oggi, la posta elettronica è sia il principale strumento di comunicazione che il principale veicolo di minacce: il 94% di tutto il malware viene infatti diffuso tramite messaggi e-mail. La sicurezza del servizio Email è quindi un fattore estremamente importante per difendersi dalle principali modalità di attacco come ransomware, spyware, worms e varie forme di attacchi di social engineering come phishing o spear phishing e altre cyber minacce.

Le Email sono quindi il principale vettore di attacco per i cyber criminali che tentano penetrare nella rete aziendale per sottrarre informazioni sensibili come le personally identifiable information (PII), protected health information (PHI) o proprietà intellettuali (spionaggio industriale).

Gli impatti del malware o degli attacchi di phishing risultano essere sempre più critici per le aziende colpite. Come sottolinea infatti il recente Rapporto Clusit 2022, il 79% degli attacchi rilevati ha avuto un impatto "elevato", contro il 50% dello scorso anno. In dettaglio, il 32% è stato caratterizzato da una severity "critica" e il 47% "alta".

In termini operativi concreti, questo significa esporsi a prolungate indisponibilità dell'infrastruttura IT ed alla possibile perdita di dati e/o della loro riservatezza, fino ad arrivare alla totale messa fuori uso dei sistemi informatici e di supporto alla produzione.

L'impatto di un attacco cyber quindi va ben oltre i costi da sostenere per eliminare il problema e ripristinare il funzionamento e dovrebbe considerare anche i costi collaterali quali la perdita di reputazione e i danni amministrativi e legali legati all'interruzione dell'operatività propria e dei clienti serviti.
Ecco perché occorre progettare e implementare un piano di difesa completo in cui la protezione della posta elettronica sia un elemento imprescindibile.
Tutto ciò se vogliamo che la posta elettronica possa continuare a rappresentare uno strumento di lavoro per tutti noi.
Sottovalutare queste considerazioni, non agire per affrontare il problema significa offrire sempre più spazio ad una minaccia concreta per il business.

Per maggiori informazioni sulle soluzioni di Mail Security cliccare sul link seguente:

https://www.digiway.it/home.nsf/contents/libraesva%20email%20security%20gateway.html

CAPITOLO DUE

Le principali tecniche di attacco utilizzate con l'email

Secondo un'analisi realizzata da LibraEsva sull'evoluzione dell'e-mail security in Italia e riportata nel rapporto Clusit 2022, emerge che le minacce si fanno sempre più subdole e che le tecniche di attacco evolvono in direzioni più difficili da monitorare, da quantificare e anche da intercettare. È fondamentale quindi che le aziende (tanto le PMI che le Enterprise):

- aumentino subito il livello di consapevolezza di tutti i propri addetti delle possibili conseguenze di un cyber attacco;
- mantengano aggiornate le cyber difese restando al passo con l'evoluzione delle tecniche di attacco.

Il problema si fa meno tecnico, più metodologico e sempre più specialistico.

Vediamo ora i principali tipi di attacco che usano le email come veicolo di trasmissione.

Gli attacchi Business E-mail Compromise (BEC) sono schemi di frode che consistono nell'impersonare un membro importante dell'azienda

destinataria. Secondo Verizon, questo tipo di frode è stato il secondo attacco, per importanza, di social engineering del 2021 e l'FBI ha aggiunto che gli attacchi BEC sono costati alle aziende statunitensi più di 2 miliardi di dollari tra il 2014 e il 2019.

L'Email Account Compromise (EAC) è un attacco altamente sofisticato in cui gli aggressori utilizzano varie tattiche, come password spray, phishing e malware, per compromettere gli account di posta elettronica delle vittime, ottenendo l'accesso a caselle di posta legittime.

L'attacco può essere lo scopo finale dell'avversario (nei casi tipici di spionaggio, ad esempio) ma può essere uno degli step di un attacco più articolato le cui finalità possono essere legate alla raccolta di informazioni o allo sviluppo di un attacco su un terzo soggetto in qualche modo legato all'account compromesso.

Non occorre essere degli esperti di informatica per comprendere come gli attacchi di tipo Email account compromise risultino utili ai criminali per diversi motivi:

1. consentono di effettuare comunicazioni verso terzi con un altissimo livello di fiducia;

2. consentono, nel caso di sviluppo di un attacco via email, di evitare i classici indicatori di compromissione di una mail, risultando dal punto di vista tecnico ed oggettivo, provenienti da una sorgente legittima;

3. forzano i sistemi di protezione della posta a concentrarsi solo sul livello di contenuto del messaggio e non su altri elementi.

I due tipi di attacco citati sono tra i più comuni ma l'evoluzione continua delle tecniche di attacco è tale che non possiamo escludere che mentre scriviamo ne stiano nascendo di nuove.

CAPITOLO TRE

- Come scegliere un Sistema di protezione delle email -

Quali sono le caratteristiche principali di un buon Email Security Gateway?

Partiamo dagli scopi: il mail security gateway deve innanzitutto bloccare le minacce informatiche prima che raggiungano il server di posta aziendale e soprattutto prima che siano consegnati nella casella postale dell'utente, il quale potrebbe rischiare di considerarli messaggi validi. Una caratteristica altrettanto importante è la capacità di operare producendo il minor numero possibile di falsi positivi.

Fra le caratteristiche principali da valutare ricordiamo:

- Indispensabile è la presenza di Sandbox proprietarie per bloccare le minacce sconosciute incorporate in link e nascoste in allegati dannosi:
- Risulta fondamentale monitorare il livello di "fiducia" tra mittente e destinatario delle email;
- Per garantire una protezione elevata è fortemente consigliato l'uso di strumenti di Intelligenza artificiale e motori di apprendimento automatico;
- Una volta identificate le minacce devono essere rimosse facilmente e rapidamente dalle caselle di posta degli utenti. Questa funzione è generalmente chiamata Threat Remediation;
- Un portale di analisi delle minacce (Threat Analysis Portal) consente agli utenti e ai responsabili della sicurezza di analizzare le minacce rilevate dal Mail Security Gateway e confrontarle con le statistiche globali;
- La crittografia email End-to-End per inviare in tutta sicurezza dati e informazioni;
- Il Mail security gateway deve integrarsi con i principali sistemi di posta elettronica come Microsoft 365™, Exchange™, Domino Notes, G Suite™, Zimbra© e molti altri mail server.
- Alta disponibilità e affidabilità con il cluster attivo-attivo;
- Molteplici motori antivirus per garantire la massima copertura.
- La segnalazione di mail provenienti dall'esterno da mittenti non ancora conosciuti.

Infine segnaliamo che risulta importante considerare il totale rispetto della normativa GDPR da parte della soluzione scelta.

Per maggiori informazioni sulle soluzioni di Email security siamo a vostra disposizione per posta elettronica all'indirizzo **commerciale@digiway.it** o via web a questo **indirizzo**.

CAPITOLO QUATTRO

- Case History -

Esperia Health Care Operations.

La Case History è disponibile sotto forma di documento pdf, che potrete scaricare collegandovi direttamente al sito del vendor, potrete toccare con mano la soddisfazione di uno dei nostri clienti più attenti alla sicurezza: un gruppo di società impegnate nella sanità privata.

CAPITOLO CINQUE

- Email archive - Norme e buona pratica

Anche se molti non ne sono consapevoli, l'archiviazione è anzitutto un obbligo di legge.

Sono numerose le normative che regolano l'archiviazione della corrispondenza aziendale via email; primo fra tutte il codice civile (art. 2214) che impone la conservazione dei messaggi di posta elettronica a rilevanza giuridica e commerciale per 10 anni, tramite appositi processi e strumenti che garantiscano qualità, sicurezza, integrità e immodificabilità del dato come previsto dalle linee guida AGID. In linea di massima, il 90% delle email è di natura non strettamente giuridica e non impegna il Titolare del trattamento secondo la ratio del Codice Civile, ma è fortemente consigliato conservare tutte le email inviate e ricevute, delle quali l'azienda è proprietaria e responsabile.

Infatti la casella di posta dovrebbe essere dedicata a un esclusivo uso aziendale; questo conferisce all'azienda il diritto di "controllarla", ma anche il dovere di gestirla rispettando la normativa, poiché la responsabilità ricade sulla direzione aziendale stessa.

In materia di gestione e archiviazione della posta elettronica, il primo passo importante da compiere è emanare un apposito regolamento aziendale, come specificato in Gazzetta Ufficiale n. 58 del 10 marzo 2007 che indichi al dipendente se l'utilizzo della propria mailbox è esclusivamente di natura lavorativa o promiscuo; in caso di regolamento assente, si dà per scontato che il suo utilizzo sia promiscuo e quindi il datore di lavoro non ha alcun diritto di conservazione.

Dando per certo che tale regolamento sia in atto, l'azienda è proprietaria della casella di posta e ha pertanto diritto ad accedere ad essa in qualsiasi momento, in presenza o meno del relativo proprietario.

Archiviare la posta elettronica, si configura anche come una buona pratica aziendale che ha lo scopo di conservare il contenuto delle comunicazioni scambiate via email e consentirne il recupero istantaneo, anche in caso di assenza del legittimo proprietario. Le email sono infatti il contenitore del know how aziendale e, pertanto, dotarsi di un sistema di archiviazione significa fornire alla memoria aziendale una parte importante delle risorse necessarie alla quotidiana operatività e tutelarsi in caso di controversie giuridiche.

Tutte queste necessità assumono ulteriore rilevanza nel momento in cui si parla di Posta Elettronica Certificata.

Nata nel 2005, la PEC si configura come un messaggio di posta elettronica avanzata che si differenzia da quelli elettronici ordinari

poiché permette al mittente di associare al messaggio la "prova legale" della sua spedizione e della sua ricezione da parte del destinatario.

Concretamente, la corretta gestione dello strumento permette di soddisfare le caratteristiche di:

- provenienza certa
- gestore terzo e qualificato
- processo certificato e qualificato secondo le regole tecniche in concreto applicabili
- sistema documentale conforme.

Dal punto di vista normativo, essendo i messaggi PEC dei documenti informatici, l'art. 43 del Codice dell'amministrazione Digitale (CAD) dispone che la conservazione degli stessi debba essere eseguita nella modalità digitale secondo le regole tecniche in materia di sistema di conservazione e, quindi:

- identificabilità certa del soggetto che ha creato il documento
- integrità del documento (attraverso l'apposizione della marca temporale)
- leggibilità e agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari rispetto delle misure di sicurezza.

Per maggiori informazioni sulle soluzioni di Email Archive siamo a vostra disposizione per posta elettronica all'indirizzo **commerciale@digiway.it** o via web a questo **indirizzo**.

HAI TROVATO QUESTO ARGOMENTO INTERESSANTE?

Puoi inviarci le tue esperienze e i tuoi commenti all'indirizzo info@digiway.it . I casi più interessanti li pubblicheremo sul nostro blog. Se invece vuoi approfondire l'argomento Email Security o valutare con i nostri specialisti il livello delle protezioni attuali nella tua azienda, siamo a tua disposizione. Scrivici un'email o chiamaci direttamente:

DIGIWAY SRL

Via Caldera, 21
Edificio Easypoint, 1° piano
+39 02 8715 8030

info@digiway.it

www.digiway.it

DIGIWAY