Posta elettronica: rischi e difese

DIGIWAY

Introduzione

Con il nostro partner Libraesva, leader italiano della mail security, abbiamo realizzato una serie di brevi articoli che abbiamo pubblicato sulle pagine del nostro blog e su Linkedin, sul tema della gestione sicura e conforme alla normativa delle email aziendali. Lo scopo è quello di 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.

In questo pdf sono raccolti tutti gli articoli pubblicati.

CAPITOLO UNO

- Account Take over - Cos'è e come ci si protegge

Cos'è l'Account Takeover? Si parla di ATo Account Takeover quando un cybercriminale ottiene il controllo (take over) di un account altrui in maniera illegittima. Il criminale informatico ottiene le credenziali di accesso dell'account della vittima, tramite brand impersonification, phishing e tecniche di social engineering ecc. e, successivamente, monitora le attività per apprendere come l'azienda fa affari, gestisce le transazioni finanziarie e molto altro ancora.

Tutto questo consente al criminale informatico di rubare informazioni preziose a scopo di estorsione o per rivenderle ai concorrenti, utilizzarle per danneggiare l'azienda, generare e

diffondere ulteriori attacchi informatici, atti ad acquisire le credenziali di accesso di altri account, dando vita a un ciclo senza fine.

Sono diverse le minacce diffuse via email che consentono ai criminali informatici di entrare in possesso delle credenziali di accesso all'account della vittima. Alla base di ognuna di queste c'è il Social Engineering, un insieme di tecniche utilizzate dai cybercriminali per profilare aziende e persone da attaccare e indurle a condividere, ignari dell'inganno, i propri dati di accesso.

Come funziona?

Il cyber criminale invia un'email che sembra, in tutto e per tutto, provenire da un brand o da un'azienda conosciuta al target che la riceve. Il grado di plausibilità e verosimiglianza dell'email è diventato molto alto e migliora continuamente. Così la vittima è indotta a condividere gli accessi del proprio account email o a fornire dati personali e sensibili come delle credenziali privilegiate.

La procedura di solito viene automatizzata ricorrendo ai bot che riempiono i campi di login dei vari siti web con le credenziali ottenute. Da qui ne conseguono furti di dati sensibili, transazioni finanziarie, acquisti fraudolenti e invio massivo di email, talune anche pericolose e contenenti ulteriori minacce.

Come difendersi?

Difendersi da questo tipo di truffe richiede di prendere in considerazione due aspetti principali.

Fattore umano

Le persone che lavorano o collaborano con l'azienda devono essere formate al fine di conoscere i rischi di queste truffe e riconoscere i segnali sospetti, come ad esempio il vostro Amministratore Delegato che vi chiede di effettuare un bonifico urgente senza ulteriori chiarimenti.

Deve essere spiegato ai collaboratori aziendali che è sempre meglio essere sospettosi di fronte a richieste strane che arrivano via email, anche se apparentemente arrivano da persone fidate.

Inoltre è necessario far capire agli utenti l'importanza di una corretta gestione delle password evitando password troppo semplici o il riuso delle stesse su più servizi.

Fattore tecnologico

In azienda devono essere adottate adeguate misure di sicurezza volte a proteggere gli account email, ed in generale qualsiasi accesso a pannelli amministrativi, mediante misure di sicurezza adeguate.

Per maggiori informazioni sulle soluzioni di account takeover protection cliccare sul link seguente:

https://www.digiway.it/home.nsf/contents/cybersecurity_intro.html

CAPITOLO DUE

- Phishing e Phishbrain -

Cos'è il phishing?

Il phishing è una particolare tipologia di attacco informatico che, tramite l'invio di email massive contenenti link o allegati malevoli a liste di destinatari disponibili nel mercato degli hacker, induce la propria vittima a fornire informazioni riservate, da parte di un soggetto che si finge affidabile.

Perché gli attacchi phishing hanno successo?

Purtroppo è molto diffuso un falso mito sulla difesa degli account email aziendali e cioè che sia sufficiente un buon Antivirus e un

qualsiasi Antispam per proteggersi da questi attacchi. Purtroppo non è così!

Gli attacchi di phishing hanno successo perché fanno leva sul fattore umano, che è la componente più debole della sicurezza di una azienda.

Le persone non prestano sufficiente attenzione alle richieste apparentemente legittime e finiscono per condividere erroneamente dati sensibili e riservati.

Perché dovresti prestare attenzione?

Oltre il 25% dei destinatari delle email di phishing clicca sul contenuto della email senza pensarci e riflettere. Oltre il 50% di questi compila form online inviando informazioni riservate e sensibili.

Quale impatto economico ha mediamente un attacco phishing?

Le più recenti analisi indicano che le violazioni costano, in media, più di 130.000 dollari e possono raggiungere i milioni, causando il fallimento di molte aziende.

È fondamentale quindi educare i propri utenti e valutarne periodicamente la consapevolezza relativa a questa metodologia di attacco.

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

CAPITOLO TRE

- Email security -

L'email è il principale veicolo di dati e informazioni aziendali e, proprio per questo, il vettore di attacco privilegiato dai criminali informatici.

Il 96% degli attacchi di Social Engineering hanno avuto inizio con un'email di phishing[1].

Gli attacchi Business Email Compromise (BEC) hanno causato perdite per oltre 1.8 miliardi di dollari[2].

Il costo medio di un Data Breach nel 2020 è pari a 4,24 milioni di dollari, il 10% in più rispetto all'anno precedente[3].

[1] Verizon, "2021 Data Breach Investigation Report

[2] FBI. Crime Complaint Center 2020 Internet Crime Report

[3] IBM Cost of a Data Breach Report 2021

I dati riportati indicano che un buon progetto di strategia di Cyberdefense non può prescindere da un ottimo sistema di difesa del servizio Email.

QUALI CARATTERISTICHE DEVE AVERE UN ECCELLENTE SISTEMA DI PROTEZIONE DEL SERVIZIO EMAIL.

- Protezione aggiornata continuamente anche dalle minacce avanzate come BEC, phishing, Brand Impersonification.
- TRASPARENZA TOTALE sul traffico email e sui contenuti malevoli bloccati, tramite TAG utili a identificare la pericolosità dell'email o il suo indice di spam.
- RICERCHE rapide, complesse e dettagliate di ogni email bloccata.
- GESTIONE CENTRALIZZATA e semplificata delle email con un'unica console.
- INSTALLAZIONE E OPERATIVITÀ rapide e immediate.
- INTERFACCIA semplice e intuitiva.
- APP MOBILE per gestire in mobilità la tua mailbox e la quarantena.

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

- Sandbox -

Cos'è un sandbox?

Nel mondo della sicurezza informatica, con il termine Sandbox si indica un ambiente di test in cui eseguire un codice nuovo o ancora non testato, al fine di analizzarne il comportamento in modo sicuro, senza rischiare di danneggiare il computer o la rete.

Questo codice a volte potrebbe essere un exploit zero-day, i cui effetti non sono ancora noti. Per questo motivo è fondamentale che le Sandbox non abbiano alcun accesso alla rete.

Le Sandbox sono indispensabili per analizzare il malware e bloccarne la diffusione prima che diventi una minaccia globale. Utilizzando le Sandbox, gli esperti di sicurezza informatica possono analizzare come

funziona il malware, quali effetti ha e poi progettare le soluzioni per renderlo innocuo.

Come agisce una Sandbox evoluta?

RESILIENZA A TECNICHE DI EVASIONE:

la Sandbox non si deve occupare solo di analizzare il comportamento di un file, ma deve essere il primo meccanismo di difesa. Deve innanzitutto bloccare attacchi sconosciuti ed evasivi disarmandoli a priori. Questo approccio la rende virtualmente immune alle tradizionali tecniche di evasione.

SANITIZZAZIONE DEL DOCUMENTO:

la Sandbox consegna solo documenti sicuri, rimuovendo il contenuto attivo sospetto o pericoloso dei documenti Microsoft Office TM, PDF e RTF, anche in archivi compressi.

La Sandbox quindi consegna il documento sanificato o blocca l'intero documento.

L'analisi viene effettuata interamente nel gateway. In questo modo, tutti i dati sono tenuti al sicuro.

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

CAPITOLO CINQUE

- Case History -

Esperia Health Care Operations.

La Casa di Cura Villa Esperia è un centro ospedaliero nel cuore delle verdi colline dell'Oltrepò Pavese, parte di un più ampio gruppo sanitario, uno dei nostri clienti più attenti alla sicurezza, che opera in nord Italia offrendo percorsi di salute personalizzati.

Villa Esperia cercava una soluzione in grado di ridurre radicalmente la superficie di attacco e il livello di esposizione alle minacce diffuse via email, per nulla tollerabile visti il tipo di servizi offerti e la particolare sensibilità dei dati gestiti.

Dopo avere analizzato e testato diverse soluzioni, alcune sviluppate anche da vendor affermati, Villa Esperia ha deciso di richiedere una

trial gratuita dell'Email Security Libraesva. Con il supporto di Digiway Srl sono stati analizzati aspetti e peculiarità del prodotto e, in brevissimo tempo, l'azienda ha deciso di adottare la soluzione a protezione delle proprie mailbox.

La Case History è disponibile al seguente link:

https://www.digiway.it/home.nsf/contents/storie%20di%20successo.html

CAPITOLO SEI

- 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