L’email non è uno strumento sicuro: dalla Business Email Compromise allo Spoofing

1.1 La Business E-mail Compromise (BEC): che cos’è e quanti danni sta causando nelle aziende

Oggi la maggior parte delle truffe informatiche sono realizzate utilizzando l’e-mail, uno strumento diffuso ma con quale risulta estremamente facile (e poco costoso) applicare le tecniche del Social Engineering e il phishing.

Tra le truffe veicolate attraverso l’e-mail, quella che oggi sta mietendo più vittime (soprattutto in termini economici!) è la Business Email Compromise (BEC). Introduciamo l’argomento raccontando un **caso reale**, accaduto a settembre 2017 e finito su tutti i giornali.

Il direttore della delegazione della Confindustria presso l’Unione Europea a Bruxelles riceve un’e-mail dalla sua superiore:

“Caro G., dovresti eseguire un bonifico di mezzo milione di euro (in realtà la cifra era leggermente inferiore, ndr) su questo conto corrente. Non mi chiamare perché sono in giro con il presidente e non posso parlare”. Mittente: M. P.

Figura 1. Dal sito di Repubblica.it (30/09/2017), http://www.repubblica.it/cronaca/2017/09/30/news/beffa_a_bruxelles_mister_confindustria_truffato_e_licenziato-

176906111/.

Il funzionario della Confindustria a Bruxelles ha eseguito il bonifico – che non avrebbe dovuto fare – e circa cinquecentomila euro sono passati da un conto della Confindustria a un conto estero di cui non si conosce l'intestatario. **Soldi evaporati**, scomparsi per sempre.

Come è stato possibile? Tutto è cominciato da una mail che era falsa, ma alla quale il funzionario ha purtroppo dato credito. E per questo è stato licenziato.

Il lettore potrebbe pensare: *"è stato uno sprovveduto, come si può cascare in una truffa del genere?"*

E invece, anche se sembra incredibile, in tantissimi ci cascano…

È successo in Confindustria ma sono centinaia le aziende quotidianamente colpite da frodi finanziarie e addirittura milioni le mail contraffatte ("mail spoofing", appunto) da cui partono ordini per spostare denaro in ogni parte del mondo.

È accaduto anche alla società calcistica S.S. Lazio, che a marzo 2018 ha pagato l'ultima rata per il giocatore De Vrij su un conto bancario diverso da quello indicato dal club olandese del Feyenoord di Rotterdam. E così, **due milioni di euro sono andati in fumo…**

Un importante rapporto redatto dal Federal Bureau of Investigation[1] (la ben nota **FBI**) del 4 maggio 2017 ci mostra i danni generati dalla BEC nel mondo.

Figura 2. Il Rapporto FBI del 4 maggio 2017

Secondo l'FBI, le truffe BEC sono state segnalate in oltre cento Paesi e hanno fatto registrare un notevole aumento, pari al 2.370%, delle perdite rilevate tra gennaio 2015 e dicembre 2016.

L’ultimo aggiornamento del Rapporto FBI sulla BEC è uscito il 12 luglio 2018[1]: il totale delle perdite è salito all’astronomica cifra di **12.536.948.299 USD** (nel periodo tra ottobre 2013 e maggio 2018). Confrontando i due rapporti scopriamo che in meno di un anno e mezzo (da dicembre 2016 a maggio 2018) sono stati persi per la BEC altri 7,2 miliardi di dollari, con un aumento del 2.200% tra il 2015 ed il 2017 e un picco massimo nel settembre 2017, con oltre 18 milioni di dollari persi in un solo mese.

Quindi, riassumendo, **l’e-mail spoofing** può servire per veicolare malware (tra i cui i famigerati ransomware), ma anche per la truffa nota come Business E-mail Compromise (BEC) e di cui il caso raccontato (verificatosi in Confindustria) rappresenta solo una delle possibili varianti, quella definita come “CEO Fraud” (la frode del CEO).

Ogni giorno, circa 400 organizzazioni sono vittime di attacchi tramite BEC, che rappresentano un enorme fattore di rischio per le aziende. E nella maggior parte dei casi vengono presi di mira addetti all’interno dello staff finanziario dell’azienda.

Il funzionamento ha le caratteristiche di una **truffa classica**, dove la tecnologia è soltanto un mezzo nuovo per portare a termine raggiri vecchi.

In genere, i cyber attacchi che sfruttano le e-mail come vettore di minacce cibernetiche al loro interno contengono allegati con malware. Con le CEO Fraud e le BEC, invece, **non ci sono allegati**, ma solo il corpo normale di un messaggio, nel quale l’attaccante cerca solo di rendersi credibile, “clonando” al meglio il mittente.

L’**obiettivo** è che la vittima riconosca il messaggio come veritiero, proveniente da una fonte certificata e autorevole. A quel punto, l’aggressore chiederà al suo bersaglio di compiere un gesto specifico, che sia un trasferimento di

denaro o fornire l’accesso a informazioni riservate. Quest’ultimo non si insospettirà, perché il messaggio non contiene allegati (considerati pericolosi). Quindi probabilmente eseguirà la richiesta, soprattutto se operazioni simili (bonifici, ecc.) avvengono già in azienda e con le stesse modalità.

1.1.1 La truffa “The Man in the Mail”

Un’altra delle varianti della BEC è la truffa definita “The Man in the Mail”.

I delinquenti intercettano la posta elettronica di un’azienda e fanno in modo che i pagamenti finiscano sui loro conti correnti. Colpisce **soprattutto aziende che fanno import/export**, in quanto il conto su cui viene dirottato il pagamento si trova all’estero (preferibilmente in paesi molto lontani e generalmente extra-europei).

Ma non solo: ultimamente ho conosciuto molti casi nei quali il conto utilizzato per la truffa era localizzato in Italia (e intestato a un ignaro prestanome). È l’evidenza di un fenomeno in forte crescita e di cyber criminali sempre più intraprendenti.

Come funziona la truffa “The Man in the Mail”?

Il malvivente viola la casella di posta, quella del mittente oppure quella del destinatario, mediante tecniche diverse ma ugualmente efficaci: phishing, social engineering, furto delle credenziali o attacco “brute force”.

Studia quindi le comunicazioni dell’azienda, la carta intestata, le firme dei responsabili, lo stile della corrispondenza. Scopre i ruoli aziendali, individuando – per esempio – chi è preposto ad eseguire i pagamenti ai fornitori.

Poi si inserisce in conversazioni già in corso comunicando, alla persona giusta dell’azienda, coordinate bancarie diverse

(le sue!) su cui eseguire i pagamenti. Per fare questo usa appunto lo “spoofing”, falsificando il mittente, oppure usando un indirizzo e-mail appena diverso, o – ancora – accedendo direttamente all’email violata.

In alcuni casi, avendo avuto accesso alla corrispondenza tra cliente e fornitore, riesce anche a richiamare numeri d’ordine o importi relativi a forniture realmente eseguite.

Il risultato è che l’azienda cliente (quella che deve pagare) si vede arrivare un messaggio credibile o addirittura contenente una fattura confezionata con la grafica uguale a quella vera (che l’hacker ha copiato), che indica di eseguire il pagamento su un conto diverso (non quello solito). E probabilmente lo eseguirà **senza farsi troppe domande…**

I numeri riportati nel citato Rapporto FBI ci fanno capire che questa truffa – se ben organizzata – ha ottime probabilità di successo.

1.1.2 Le varianti della Business Email Compromise

Questa frode si sviluppa in svariate modalità: sono classificate nel citato Rapporto FBI, che indica cinque differenti scenari (ove i primi due sono i più diffusi):

1. **Business tra cliente e fornitore**: richiesta di pagamento con e-mail falsificata. Viene definita – come sopra spiegato – “The Man in the Mail” e anche “Bogus Invoice Scheme” “Supplier Swindle” o “Invoice Modification Scheme”.
2. “**CEO Fraud” o “Business Executive Scam”**: una richiesta di bonifico bancario viene inviata dall’account compromesso di un dirigente aziendale di alto livello (CEO o Chief Financial Officer) a un dipendente all’interno dell’azienda, che è in genere responsabile dell’elaborazione di tali richieste. È la variante di

phishing definita anche “whaling”, perché punta al “pesce grosso”.

3. **Business Contacts through Compromised E-mail**: un dipendente di un’azienda ha la sua e-mail personale violata. Questa e-mail personale può essere utilizzata per comunicazioni personali e aziendali. Le richieste di pagamenti di fatture a conti bancari controllati da frodi vengono inviate dall’e-mail personale di questo dipendente a più fornitori, identificati dall’elenco dei contatti di questo dipendente.
4. **Business Executive and Attorney Impersonation**: le vittime vengono contattate da truffatori che di solito si identificano come avvocati o rappresentanti di studi legali e sostengono di trattare questioni riservate o urgenti. Le vittime possono essere spinte dal truffatore ad agire rapidamente o segretamente nella gestione del trasferimento di fondi. Questo tipo di truffa BEC può verificarsi alla fine della giornata o della settimana lavorativa ed essere programmata per coincidere con la chiusura delle attività delle istituzioni finanziarie internazionali.
5. **Data Theft** (furto di dati): le richieste fraudolente vengono inviate utilizzando l’e-mail compromessa di un dirigente. I destinatari della richiesta sono figure dell’organizzazione aziendale che conoscono dati importanti, come risorse umane, contabilità o auditing. Queste richieste, in genere, si verificano prima di una richiesta fraudolenta di bonifico bancario.

1.1.3 Come difendersi dalla Business E-mail Compromise

Esaminiamo ora come proteggerci da queste frequenti e temibili truffe.

Come sempre è importante avere la consapevolezza (“awareness”) del rischio e non sottovalutarlo. Vediamo quindi quali sono

gli **accorgimenti** da adottare in azienda:

- Usare credenziali di accesso alle mail robuste e sicure, quindi impostare una corretta gestione delle password.
- Non utilizzare in azienda indirizzi e-mail basati su webmail, perché sono più facilmente accessibili ed attaccabili.
- Leggere le mail con attenzione, soprattutto quelle che si riferiscono a pagamenti. Nel dubbio, fare verifiche con mezzi diversi. È cioè molto importante non chiedere la conferma usando lo stesso indirizzo, perché ci risponderebbe il truffatore. Usare piuttosto il telefono, o contattare direttamente il mittente utilizzando l'indirizzo presente nella rubrica aziendale oppure un altro indirizzo e-mail, della cui credibilità siamo certi.
- Controllare bene il mittente delle e-mail: un dettaglio (anche solo una lettera!) potrebbe fare la differenza. Alcuni esempi di come è facile indurre in inganno con un indirizzo e-mail modificato ad arte: l'e-mail reale info@pippodomus.com potrebbe essere trasformata dal truffatore in: info@pippodornus.com. La sostituzione della lettera "*m*" con "*rn*" è difficilmente distinguibile a colpo d'occhio (e chi legge l'e-mail va sempre di fretta…). Oppure potrebbe essere modificata in info@pipp0domus.com sostituendo la lettera "o" con il numero "0", pressoché identico. O anche: info@pippo-domus.com (un segno meno che passerà facilmente inosservato). E molte altre: l'inventiva degli attaccanti è illimitata…
- E soprattutto: evitare di pensare "figurati se una cosa del genere può succedere a me". Può succedere a chiunque, se non si è attenti e consapevoli.

In altre parole: come sempre, è il **fattore umano** che può fare la differenza.

1.2 Come funziona la posta elettronica e perché è insicura

La BEC, come abbiamo illustrato, è resa possibile grazie al basso livello di sicurezza della posta elettronica.

L'email non è che una delle molte modalità di utilizzo di Internet. È stata una delle prime, creata alla nascita di Internet, e proprio in questo risiede la sua **intrinseca debolezza.**

La sua invenzione risale infatti al **1971**, quando Ray Tomlinson installò su ARPAnet un sistema in grado di scambiare messaggi fra alcune università americane e inviò la prima e-mail. Cosa c'era scritto in quella e-mail? Ray Tomlinson disse di non ricordarlo, ma che probabilmente era una semplice scritta: "QWERTYUIOP" o qualcosa di simile.

Un'altra curiosità: fu proprio Tomlinson a scegliere il **simbolo @** per collegare username e dominio e-mail.

Successivamente, nel 1982, fu creato il protocollo SMTP (Simple Mail Transfer Protocol), ancora oggi universalmente utilizzato: tutte le e-mail spedite su Internet vengono trasferite usando questo protocollo in uscita.

Figura 3. Come funziona la posta elettronica

SMTP rappresenta l'esempio più evidente di come uno strumento creato quasi per gioco, quindi senza particolare attenzione alla sicurezza, oggi gestisce e controlla tutte le attività della nostra società.

Infatti, quando fu inventata l'email, questa fu pensata come **"strumento collaborativo"**.
La **sicurezza** non era un requisito ritenuto importante, quindi le caratteristiche dell'e-mail erano:

- Nessuna autenticazione del mittente;

- Nessuna riservatezza del contenuto;
- Nessuna verifica di integrità lungo il percorso;
- Nessuna protezione contro messaggi indesiderati.

Per questo, oggi tutti noi usiamo l'e-mail, senza pensare che si tratta di uno degli strumenti più antiquati e vulnerabili della rete.

Il protocollo SMTP è quindi uno dei più vecchi di Internet ed è volutamente mantenuto semplice, visto che un server SMTP deve poter gestire decine di connessioni al secondo. **Questa semplicità si traduce in vulnerabilità**, perché le due informazioni identificative che il server mittente passa al destinatario (il nome del mittente e l'indirizzo e-mail a cui il messaggio è diretto) non vengono verificate e possono essere quindi facilmente falsificate.

L'e-mail può essere intercettata e letta da un malintenzionato: il cosiddetto "*Man in the middle*" che si frappone tra mittente e destinatario. Infatti, nella maggior parte dei casi, le e-mail vengono trasmesse non criptate, come se fossero state scritte su una cartolina (che tutti possono leggere!).

Abbiamo detto che tra le molte limitazioni del protocollo SMTP c'è quella che **non è in grado di gestire l'autenticazione** del mittente. Questo è probabilmente la vulnerabilità più grave, perché viene sfruttata da chi usa l'e-mail come strumento di attacco per fare phishing.

È infatti possibile – e anche abbastanza facile! – inviare e-mail **falsificando il mittente**.

In altre parole: si può spedire un'e-mail facendo apparire come mittente l'indirizzo corrispondente ad un altro account. Questo anche senza avere accesso all'account falsificato, cioè senza conoscere le credenziali della casella di posta che si usa.

Questa tecnica si chiama ***spoofing*** ed è estremamente pericolosa, realizzabile senza grandi competenze informatiche e – ahimè – estremamente efficace.

1.3 Cos'è lo Spoofing?

È una tecnica di attacco utilizzata per **falsificare diverse informazioni**, come ad esempio l'identità di un host (computer o server connesso in rete) o il mittente di un messaggio. Una volta che un attaccante riesce ad impersonare qualcun altro all'interno di una rete, gli è possibile intercettare informazioni riservate, diffondere informazioni false e tendenziose o effettuare qualsiasi tipo di attacco. Risulta **particolarmente efficace combinata a tecniche di social engineering** per ottenere l'accesso a informazioni "riservate" e credenziali degli utenti. Social media scammers (truffatori) o phishers possono usare questa tecnica, ad esempio, per convincere un utente a connettersi a un server malevolo intercettando così le sue credenziali, o ad eseguire azioni dannose.

Nonostante lo spam e lo spoofing siano ancor oggi una grave vulnerabilità della posta elettronica, non si ritiene praticabile una revisione radicale del protocollo SMTP, per via del gran numero di implementazioni di questo protocollo e, soprattutto, per la complessità e il costo che comporterbbe una tale modifica.

La tecnica dello spoofing è molto efficace per realizzare attacchi di phishing e soprattutto di spear phishing, che sono diventati gli strumenti di attacco più diffusi, sia a livello privato che aziendale.

Proviamo a pensare cosa potrebbe succedere se ricevessimo un'e-mail proveniente (in apparenza!) da un collega, da un superiore o da un amico. Se questa e-mail è ben confezionata e resa credibile con riferimenti personali o aziendali, sarà abbastanza probabile che il destinatario (la "vittima"

dell’attacco) cada nel tranello e apra l’allegato, clicchi sul link o esegua l’indicazione riportata nel messaggio. E, molto probabilmente, non sarà neppure stata bloccata dall’antispam, proprio perché costruita con cura.

PRECISAZIONE: nel caso in cui l’attaccante sia riuscito a ottenere la password della casella di posta, le e-mail di phishing vengono inviate dalla casella originale che è stata violata e non da un indirizzo fittizio. In questo caso si tratta di **Violazione della casella** e non di **E-mail Spoofing**.

Questo caso è ancora più grave, perché significa che qualcuno sta usando la nostra casella a nostro nome e che, addirittura, potrebbe cambiare la password e impedirci di accedere alla nostra casella. Siamo già nel caso – ancor più grave – del “furto di identità”.

1.4 Gli strumenti informatici per proteggersi dallo spoofing

Gli attacchi di phishing, soprattutto se mirati (spear phishing) sono difficili da prevenire e rilevare. **Manca l’oggetto della minaccia cibernetica:** un link malevolo, un malware, ecc… quei segnali che i normali programmi antispam o antivirus sono in genere in grado di rilevare.

Inoltre, a causa della citata debolezza del protocollo SMTP e al fatto che i principali client di posta elettronica mostrano solitamente solo il nome del mittente, è complicato per chi riceve i messaggi capire che si tratta di un inganno.

In realtà, le e-mail di spoofing lasciano sempre qualche traccia, ma per vedere l’indirizzo reale del mittente (o quanto meno il server da cui è partita) bisogna compiere alcune azioni, che l’utente medio non conosce e che solo chi ha una certa esperienza di informatica riesce a mettere in pratica.

Quando si sospetta la ricezione di messaggi contraffatti, il modo migliore di verificarne la reale identità del mittente sarebbe quello di leggere le informazioni contenute nell'header dell'e-mail ricevuta.

1.4.1 Leggere l'HEADER di un messaggio di posta

L'header contiene le intestazioni del messaggio stesso e ha al suo interno le **informazioni relative a tutta la storia dell'e-mail**, dal momento in cui viene inviata all'accettazione da parte del server destinatario, oltre alle informazioni che riguardano l'autore del messaggio stesso.

Tutti i client che usiamo per la posta elettronica (es. Outlook o Thunderbird) hanno l'opzione per visualizzare l'header di un'e-mail ricevuta. Il comando in genere si chiama "Mostra intestazioni", o qualcosa di simile. Attivando il comando, potremo accedere alla parte "nascosta" dell'e-mail e visualizzarne molti dettagli.

Per esempio: il campo "*Received From*" indica il server mittente, da cui è partito il messaggio (questa informazione potrebbe svelarci lo spoofing).

In realtà, saper leggere l'header di un'e-mail **non è facile** e non si può pretendere che lo faccia un normale utente, senza specifiche competenze IT.

1.4.2 Una Email sicura: come ottenerla?

Rendere più sicuro un sistema progettato nativamente in modo totalmente insicuro, qual è SMTP, non è semplice.

Sono stati creati – a posteriori – metodi di controllo per prevenire lo spoofing e validare i messaggi di posta. Si tratta di:

- **Sender Policy Framework (SPF)**: consente di verificare

che una e-mail inviata da un dato dominio arrivi effettivamente da uno degli host abilitati dai gestori del dominio stesso.
- **DomainKeys Identified Mail (DKIM)**: permette ai gestori di un dominio di aggiungere una firma digitale tramite chiave privata ai messaggi di posta elettronica. DKIM aggiunge quindi un ulteriore strumento per verificare la corrispondenza tra mittente e relativo dominio di appartenenza. DKIM e SPF non sono due tecniche alternative ma piuttosto complementari.
- **Domain-based Message Authentication, Reporting and Conformance (DMARC)**: è un sistema di validazione dei messaggi di posta elettronica. Le caratteristiche di DMARC sono state definite nella RFC 7489 del marzo 2015.

Questi sistemi di controllo sono implementati nei software antispam più avanzati e moderni, che quindi possono eseguire in automatico quelle verifiche che l'utente medio – come detto – non sarebbe in grado di fare da solo.

Non basta, tuttavia, installare antispam dotati di questi sistemi: occorre anche configurare SPF, DKIM e DMARC nel modo corretto. In caso contrario si rischia che siano inefficaci o che – viceversa – blocchino anche le e-mail lecite. Aggiungiamo, in conclusione, che affinché la loro efficacia sia massima, dovrebbero essere implementate sia dal mittente che dal destinatario.

Note

[1] https://www.ic3.gov/media/2017/170504.aspx.

[2] https://www.ic3.gov/media/2018/180712.aspx.

Bibliografia e sitografia

Giorgio Sbaraglia: *"Cybersecurity kit di sopravvivenza. Il web è un luogo pericoloso. Dobbiamo difenderci!"*, GoWare, 2018.

Articolo a cura di **Giorgio Sbaraglia**

Giorgio Sbaraglia, ingegnere, è Information & Cyber Security Advisor e svolge attività di consulenza e formazione per la sicurezza informatica, Risk Management e per il GDPR.

Tiene corsi su questi temi per molte importanti società italiane di formazione, tra le quali la Business School de Il Sole 24 Ore.

È membro del CLUSIT (Associazione Italiana per la Sicurezza Informatica) e certificato “Innovation Manager” da RINA.

Ricopre l’incarico di DPO (Data Protection Officer) per alcune aziende italiane.

È autore dei libri:

“GDPR kit di sopravvivenza” (Editore GoWare) e “Cybersecurity kit di sopravvivenza. Il web è un luogo pericoloso. Dobbiamo difenderci!” (Editore GoWare)

www.giorgiosbaraglia.it

https://www.ictsecuritymagazine.com/articoli/lemail-non-e-uno-strumento-sicuro-dalla-business-email-compromise-allo-spoofing/