31 ottobre 2020

HACK IN BO Winter 2020 Edition
15ª EDIZIONE

L'avvocato ficcanaso

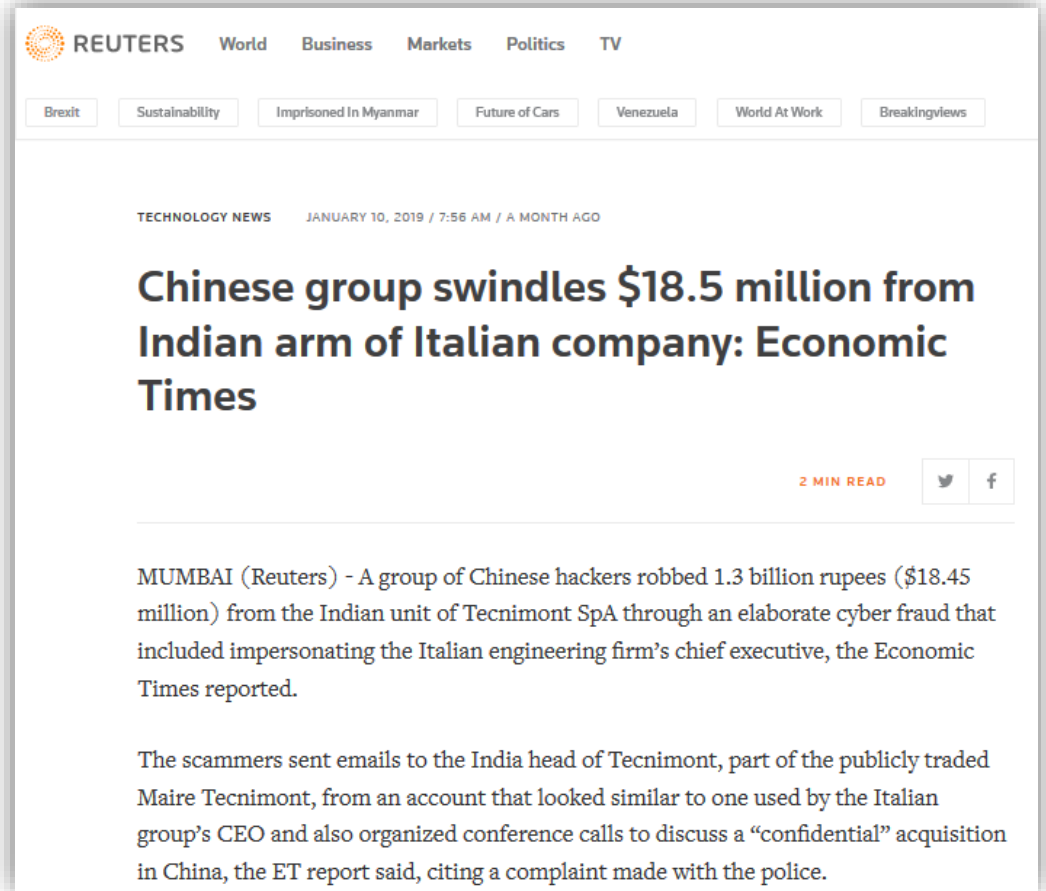
Prof. Avv. Barbara Indovina

FORENSICA

Alert e Spoiler

- I fatti e/o le vicende narrate sono realmente accadute
- Nessun Amministratore delegato è stato maltrattato
- I nomi e le città sono inventate
- No, non è stato il maggiordomo!

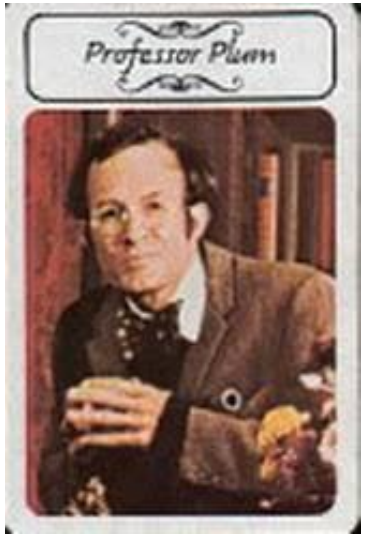
SPOILER ALERT



HACK IN BO® Winter 2020 Edition
15ª EDIZIONE

I personaggi della vicenda

La signora Fiammetta Bianchi è Amministratore delegato della società Candelabro SpA con sede in Paperopoli;



Il professor Plumb è l'amministratore delegato della Chiaveinglese SpA con sede in Topolinia (la capogruppo è irlandese) che ha appena acquisito la Candelabro SpA;

La Signora Marta Pavone e il colonnello Mustard sono due dirigenti della Chiaveinglese SpA che lavorano da tempo con la signora Bianchi (area commerciale).

Sono contattata dal Prof. Plumb che mi riferisce:

- Di aver appena terminato l'operazione di acquisizione della Candelabro SpA;
- Che nei giorni del «closing» la signora Bianchi, AD della Candelabro, aveva fatto 2 bonifici di 100.000 $ (la valuta sceglietela voi ☺) ad una società mai sentita prima con sede a Hong Kong;
- La signora Bianchi è un AD di esperienza ma è stata vittima di una truffa e ha denunciato l'accaduto alla Polizia Postale

Indagini preventive e ausilio di un CTP

Art. 327-bis c.p.p. 1. Fin dal momento dell'incarico professionale, risultante da atto scritto, il difensore ha facoltà di svolgere investigazioni per ricercare ed individuare elementi di prova a favore del proprio assistito, (…).

2. La facoltà indicata al comma 1 può essere attribuita per l'esercizio del diritto di difesa, **in ogni stato e grado del procedimento**, nell'esecuzione penale e per promuovere il giudizio di revisione.

3. Le attività previste dal comma 1 possono essere svolte, su incarico del difensore, dal sostituto, da investigatori privati autorizzati e, quando sono necessarie specifiche competenze, **da consulenti tecnici**.

Art. 391-nonies c.p.p. 1. L'attività investigativa prevista dall'art. 327-bis c.p.p., con esclusione degli atti che richiedono l'autorizzazione o l'intervento dell'autorità giudiziaria, può essere svolta **anche dal difensore che ha ricevuto apposito mandato per l'eventualità che si instauri un procedimento penale.**

2. Il mandato è rilasciato con sottoscrizione autenticata e contiene la nomina del difensore e l'indicazione dei fatti ai quali si riferisce.

Premessa: la CT nel Codice del 1930

Il Codice del 1930 era di stampo «inquisitorio», incentrato sulla «presunzione di reità» e sull'iniziativa probatoria d'ufficio. In tema di Consulenza Tecnica, ne derivava che:

- solo la parte privata poteva nominare il CT;
- il PM si poteva avvalere solo del perito nominato dal giudice istruttore;
- non esisteva la consulenza tecnica al di fuori della perizia;
- Limitato ruolo del CT e sostanziale diffidenza verso il suo operato;
- le risultanze peritali prevalevano su quelle della CT di parte.

Il Codice del 1988: la «parità delle armi»

Il «nuovo» Codice di Procedura Penale del 1988 incarna un modello tendenzialmente accusatorio:

- il PM assume il ruolo di parte;
- è sottratto al giudice il potere di compiere indagini e si attribuisce alle parti il monopolio delle attività investigative;
- il dibattimento è la sede di formazione della prova nel contraddittorio tra le parti

DIRITTO DI DIFENDERSI PROVANDO

La Difesa deve essere in grado di contrastare gli argomenti raccolti dalla Pubblica Accusa, anche avvalendosi di un proprio **CONSULENTE TECNICO.**

Parità delle armi?

CORTE DI CASSAZIONE PENALE,
Sez. 3^, 29 Maggio 2020, Sentenza n.16458

A fronte di apprezzamenti tecnico scientifici forniti dal consulente del PM non intrinsecamente illogici o contraddittori e in sé non inattendibili, e comunque non specificamente confutati dal consulente della difesa, il giudice non è tenuto, come del resto si desume dal combinato disposto degli artt. 224 e 508 cod. proc. pen., a disporre alcun accertamento peritale, del tutto inutile per l'accertamento dei fatti e per la speditezza del processo. Sicché, proprio in ragione della funzione ricoperta dal Pubblico Ministero, nell'ambito della dialettica processuale, **gli esiti degli accertamenti e delle valutazioni del consulente nominato ai sensi dell'art. 359 cod. proc. pen. rivestono, non essendo portatore di interessi di parte, una valenza probatoria non comparabile a quella dei consulenti delle altre parti del giudizio.** Pertanto, non può prescindersi dal ruolo precipuo rivestito dall'organo dell'accusa e dal suo diritto/dovere di ricercare anche le prove a favore dell'indagato, come stabilito dall'art. 358 c.p.p.: se è vero che il consulente viene nominato ed opera sulla base di una scelta sostanzialmente insindacabile del pubblico ministero, in assenza di contraddittorio e soprattutto in assenza di terzietà, è tuttavia altrettanto vero che il pubblico ministero ha per proprio obiettivo quello della ricerca della verità – concretamente raggiungibile attraverso una indagine completa in fatto e corredata da indicazioni tecnico scientifiche espressive di competenza e imparzialità – dovendosi necessariamente ritenere che il consulente dallo stesso nominato operi in sintonia con tali indicazioni.

La signora Bianchi ha già sporto querela in Questura a Topolinia in data 8.11.2020

Ehm… non proprio. Ne ha fatte 2 di querele!

1) Dettaglia l'episodio di phishing (pagamenti avvenuti il 4.11.2020 intorno alle ore 12.00);
2) Denuncia il furto del suo PC mentre da Topolinia andava alla sede di Paperopoli (sul treno) il 4.11.2020 (furto tra le 9.30 e le 10.30)

Cosa denuncia in relazione al Phishing la signora Bianchi?

- Di aver ricevuto i primi contatti da parte della collega Pavone una settimana prima- 29 ottobre 2020;
- Di non essersi accorta che in realtà la mail non era della sig.ra Pavone, persona con cui lavora da tanto e per la quale nutre stima;
- Che la (finta) Pavone le aveva detto che stava gestendo una posizione estremamente confidenziale con il Colonnello Mustard e che la avrebbe contattata un avvocato di Ginevra per spiegarle tutto (avv. Giorgetti);
- Che **avrebbero gestito tutto con mail personale e non aziendale (data la riservatezza dell'operazione)**

L'aggancio

POLIZIA DI STATO
COMPARTIMENTO POLIZIA POSTALE
E DELLE COMUNICAZIONI
EMILIA ROMAGNA

Bologna 20 dicembre 2018

OGGETTO: Segnalazione tentativo di frode informatica da diramare alle aziende associate.

Nel corso dell'attività Istituzionale svolta da questa Specialità, è emerso che un'organizzazione criminale, verosimilmente operativa in ambito internazionale, sta ponendo in essere azioni fraudolente attraverso mail, atte a trarre in inganno chi riveste l'incarico di manager o dirigente aziendale, con il fine di portare a termine una Frode Informatica.

In particolare, si tratta di una forma di truffa che viene perpetrata secondo il seguente ricorrente modello di massima:

a) ad un dirigente aziendale vengono inviate email create appositamente così da sembrare provenienti dai vertici della società o "capogruppo", ossia da soggetti sicuramente sovra ordinati nell'organigramma aziendale, rispetto al destinatario del messaggio di posta elettronica;

L'indirizzo appare corretto!

martedì 10:14

signorapavone@chiaveinglese.com ciupa@fastmail.tk>

Urgente

A

In realtà non è così…

Fiammetta sei in ufficio?
Marta Pavone

Inviato da iPhone

Segue…

b) con la falsa email viene artatamente chiesta al dirigente la piena ma riservata collaborazione per l'avvio di operazioni finanziarie o di mercato, per le quali è necessario movimentare ingenti fondi;

c) con le stesse email artefatte, il dirigente viene indotto al contatto telefonico diretto ovvero a mezzo posta elettronica, con un finto rappresentante legale segnalato come colui che gestirà, di fatto, la pratica;

Oggetto R: Urgente

No. Non ho ricevuto nessun contatto
Ciao

Inviato: martedì
Oggetto: Urgente

Sto gestendo una pratica estremamente confidenziale direttamente con Xxxxx, posso parlarne solo per email.

Ti ha contattato lo studio legale Giorgetti da Ginevra?

Marta

d) il finto legale rappresentante, infine, fornisce al dirigente aziendale vittima del raggiro, gli estremi di un conto corrente situato ad Hong Kong dove versare le somme che di volta in volta vengono richieste.

Oggetto Urgente

Nessuno in azienda deve percepire ciò che sta succedendo e parlarne è troppo rischioso. Scrivimi sulla mia email privata che ti spiego la situazione nel dettaglio.

Marta.pavone.casa@gmail.com

P.S. Alberto Giorgetti aspetta una tua chiamata: +41 22 xxx xxxx

Marta

La signora Bianchi a questo punto cosa fa?

…..Fa una telefonata alla signora Pavone di conferma (no, troppo facile avremmo già finito la presentazione)…

1. Chiama (l'inesistente) avvocato Giorgetti;
2. L'avvocato Giorgetti illustra la segretissima operazione commerciale con una società esterna e chiede di bonificare 800.000,00$ alla società GASTONE LDT con sede a Hong Kong;
3. Anche le mail della sig.ra Pavone fanno sapere alla Bianchi che tutta l'azienda conta su di lei di mantenere il massimo riserbo.
4. E lei? Lo mantiene e **paga quel che c'è sui conti**…il 4.11 alle ore 12.07

Tre ambiti di indagine:

1) **Attività ispettiva** al fine di identificare i sistemi, analizzare i processi e le persone coinvolte nel fatto anche per escludere qualsiasi coinvolgimento (volontario) di dipendenti o soggetti apicali di Candelabro SpA;

2) **Attività tecnica** al fine di acquisire le tracce e le evidenze informatiche con adeguate tecniche di computer forensics al fine di prevenire qualsiasi tipo di contaminazione nella catena di custodia del reperto anche al fine di poterle esibire in giudizio avanti al Tribunale;

3) **Attività investigativa** sui reperti e sui documenti acquisiti per verificare (ove possibile) le cause dell'incidente al fine di presentare (o integrare) atto di denuncia querela da presentare alla competente Procura della Repubblica e, eventualmente, per procedere poi ad una revisione dei processi interni all'azienda (audit) al fine di prevenire in futuro il succedersi di eventi analoghi.

Iniziamo:

Acquisiamo il pc in uso alla signora Bianchi (PC n.2) che però è nuovissimo (consegnato il 6.11 nella sede di Topolinia) a seguito del furto e ne facciamo copia forense.

Esiti

Il portatile è risultato pressoché inutilizzato: non sono stati rinvenuti elementi relativamente a webmail, comunicazioni in chat, navigazione web e interrogazioni su motori di ricerca utili ai fini della risposta al quesito. Nessun documento di lavoro né segni di attività utente, se non l'impiego della posta elettronica.

Il portatile ha mostrato segni d'uso da parte della sig.ra Bianchi unicamente per il giorno 6/11/2020 Era altresì presente un accesso il 19/11/2020 riconducibile a tecnico Candelabro Spa

Era presente un archivio di posta OST, le mail rinvenute (a volte incomplete visto che il file OST è di tipo cache) sono comprese nell'arco temporale 13/07/2020- 11/11/2020

Il supporto è risultato pressoché inutilizzato, l'analisi delle shellbags, dei file LNK, delle jump lists e del file di journal non ha prodotto risultati, alcuni registri sono risultati perfino vuoti.

Dalle mail (poche) scopriamo che:

1. La Candelabro SpA proprio nei giorni dei primi contatti del Phisher aveva proposto alla Sig.ra Bianchi di **concordare delle «dimissioni»** che lei aveva rifiutato di firmare;
2. La signora Bianchi effettua i bonifici il 4.11.2020 e si mette in malattia i due giorni successivi (su richiesta della finta Pavone);
3. Alcuni colleghi della Bianchi avevano segnalato il pagamento ma si erano accontentati di una generica risposta via mail «vi spiego tutto appena riesco»

(Il prof. Plumb non aveva mai menzionato tali circostanze)

Acquisiamo i tabulati telefonici (solo in uscita ovviamente)

- Troviamo le chiamate con il numero Svizzero;
- Redigiamo una time line degli eventi (mail e telefonate);
- Verifichiamo gli spostamenti della sig.ra Bianchi il giorno del pagamento e del furto del PC (FrecciaBlu del 4.11.2020 – in ritardo di 15 minuti alla stazione di Topolinia);
- Mail tra la Bianchi e il marito che fanno emergere che la stessa fosse arrabbiata con l'azienda e in crisi perché la volevano «fare fuori»;
- Chiediamo le telecamere della sede di Paperopoli dove la Bianchi aspettava l'avv. Paoletti il 6.11.2020 per comunicare a tutti dell'operazione (da qui si accorge della truffa e avvisa)-> troppo tardi non ci sono

Alcune mail inviate dalla Bianchi prima del phishing:

Carissimi
Da questa mail ho capito che, essendo all'oscuro di tutto, probabilmente non sono piu considerata strategica nl'evoluzione dei processi di Candelabro Spa
Preso atto domani procedo con la formale comunicazione a tutta la struttura del ruolo di Pippo , informando tutto il personale di Candelabro fare riferimento direttamente a lui per l'organizzazione delle attività.
Sono molto contenta di liberarmi di questa responsabilità e sono certa che Pippo saprà guidare le operation di Candelabro Spa modo migliore.
In tal modo potrò giustamente dedicarmi agli obiettivi strategici aziendali più consoni alla mia posizione.
Buon we
F

TARGET

E subito dopo la finta signora Pavone

Fiammetta

Mustard mi ha aggiornata.
L'unica via di uscita che vedo e' quella di procedere oggi stesso con il pagamento di 885,000.00 EUR firmanti te e Pippo , delegato da te.
E' importante che gli spieghi la sensibilita' del progetto, non voglio avere nessun tipo di comunicazione a riguardo con lui, non posso permettermi questo rischio, mi fido solo di te.
In estremis, e solo in caso di urgenza, se Pippo dovra' comunicare con me, gli fornirai questa email.

Come ben sai siamo nel bel mezzo di molti cambimenti, questa acquisizione, e la piu importante mai fatta dal gruppo e non possiamo deludere nessuno.
L'Irlanda conta molto su di me, ed io su di te, mi raccomando la confidenzialita'.
Attendo un tuo riscontro.

A

Perfetto,
Provo a spiegarti la situazione qua almeno capisci di cosa abbiamo bisogno.

Mi raccomando cancella questo messaggio dopo aver letto le informazioni che sto per darti.

Problemi

1) Candelabro SpA non ha adottato alcuna procedura circa la consegna e la restituzione di beni aziendali in uso ai propri dipendenti: non è stato possibile, quindi, avere alcun verbale che attestasse l'avvenuta consegna del computer sostitutivo alla Sig.ra Bianchi;
2) neanche in relazione al furto non vi sono documenti ufficiali che attestino la perdita dell'asset né tantomeno alcuna policy o procedura relativa a procedure di controllo da remoto sui terminali smarriti o rubati (Mobile Device Managment);
3) Il CISO è appena arrivato non ha controllo su nulla;
4) La capogruppo è irlandese e il server delle mail è allocato lì e gestito da loro (riservatezza?)

E ancora:

2) Criticità sul comportamento della signora Bianchi:

a) Lettura delle mail con la dirigenza (volevano farla dimettere e sentimento di malanimo nei confronti della azienda);
b) Smarrimento sospetto del PC
c) Si mette in malattia proprio per 48 ore (tempo della revoca del bonifico)
d) Si accorge della truffa solo 48 ore dopo aver fatto i pagamenti quando ha appuntamento con l'avv. Giorgetti (che ovviamente non arriva)

Cosa è chiaro:

C’è stata una attività intensa di *spoofing* (almeno per un mese): hanno colpito l’elemento debole sapendo tantissime cose sulla azienda e qual fosse l’anello debole come colpirlo e tramite CHI colpirlo;

Non è stato possibile effettuare nessun accertamento in relazione al PC portatile: abbiamo fatto richiesta di ottenere esistenza di log a sistemi Candelabro SpA (es. *file server*, gestionali, mail) che contenessero dati sull’IP e/o sul MAC address e/o nome macchina. (non ci hanno risposto)

Nostre raccomandazioni all'azienda:

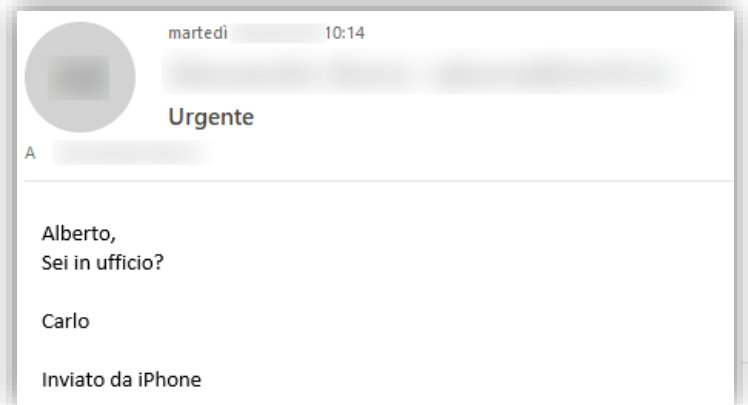
- Le risultanze investigative hanno permesso di evidenziare una serie di criticità sia tecnico-procedurali che organizzative in seno all'azienda, relative alle **procedure informatiche** in essere.
- Le attività investigative hanno subito rallentamenti e limitazioni a causa di problemi sicuramente contingenti – quali il riassetto societario e la frammentazione degli asset (Topolinia/Paperopoli/Irlanda)
- In tema di prevenzione si evidenzia come, in relazione ai fatti oggetto della odierna analisi, non vi sia stata adeguata formazione in particolar modo dei soggetti apicali (Non è in alcun modo accettabile che un Amministratore Delegato utilizzi la propria casella di e-mail personale in relazione a comunicazioni inerenti all'azienda)
- Mancano sistemi di SIEM

E ancora:

Appare doveroso effettuare una analisi più approfondita volta a stabilire se vi sono state (e sono ancora presenti) vulnerabilità in seno all'azienda ed eventuali compromissioni di sistemi (e protocolli ex D.Lgs 231/2001)

Allo stato il rischio di subire ulteriori attacchi appare verosimile.

E infatti… due giorni dopo:


martedì 10:14

Urgente

A

Alberto,
Sei in ufficio?

Carlo

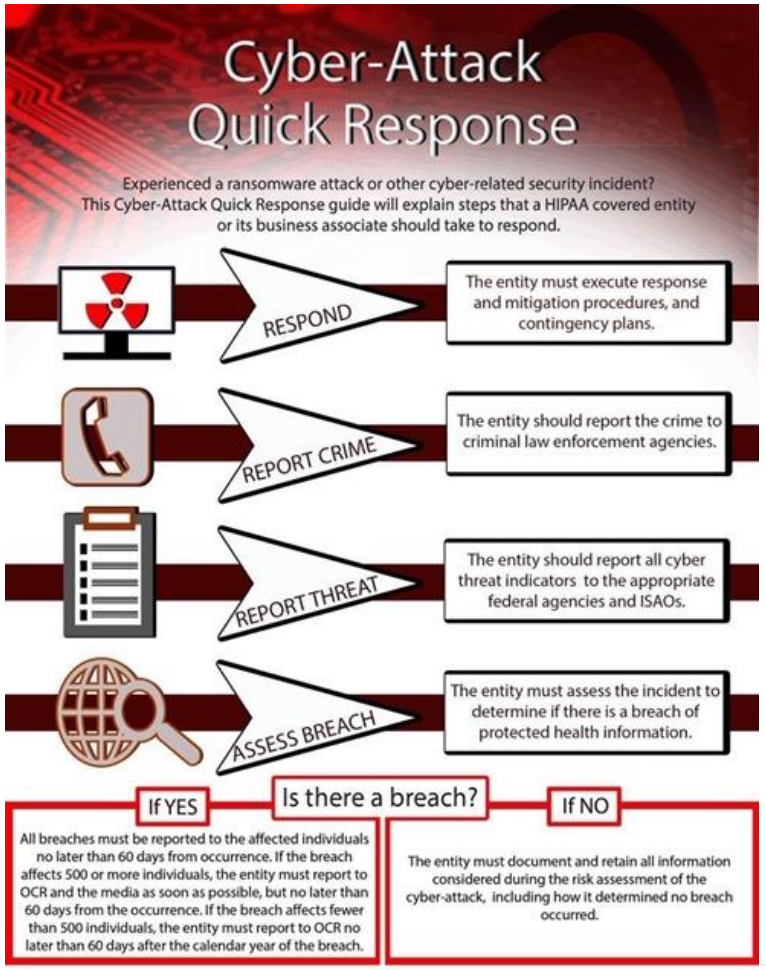
Inviato da iPhone

Gestione dell'incidente informatico, si dovrebbe…

gestire l'incidente informatico in funzione della business continuity e della collezione probatoria delle evidenze informatiche, secondo un piano già definito

- ricostruire le cause
- determinare le origini
- quantificare i danni
- fornire gli elementi necessari

per la tutela anche giudiziaria del patrimonio aziendale informatico



Ma in verità...

Il grosso delle violazioni non viene denunciato. Possibili cause:

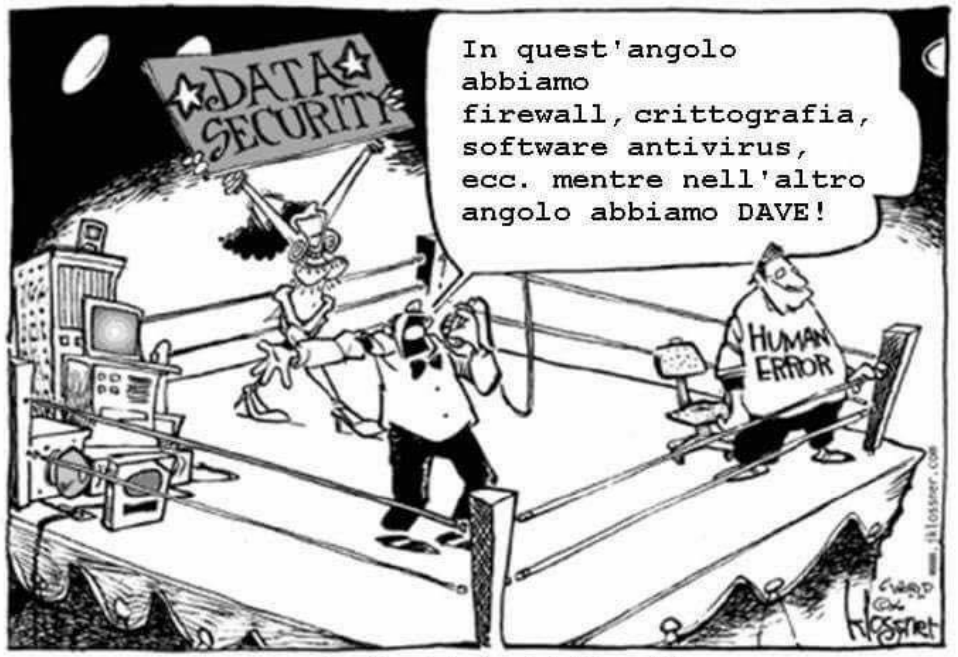
- La compromissione non viene rilevata
- Il problema viene "rattoppato" senza indagare ulteriormente
- L'indagine rimane interna all'organizzazione che ha subito la violazione
  - Timore di danno d'immagine
  - Scarsa fiducia o mancanza di interesse in un'azione legale

Perché succedono casi come questi?

- non percezione del pericolo
- fiducia delle relazioni (mail)
- assenza di procedure aziendali
- debolezza delle relazioni aziendali
- assenza di responsabilità
- mancata formazione
- assenza di sistemi di *intrusion detection*
- carenza di controlli di sicurezza informatica

→ persona

→ sicurezza perimetrale



https://www.facebook.com/vitadainformatici/

la sicurezza non è un prodotto ma un **processo** e la miglior protezione è la **conoscenza**

Bruce Schneier, crittografo, 2000:

«Solo i dilettanti attaccano le macchine; i professionisti prendono di mira le persone»

Quale reato? TRUFFA (nessun reato informatico «proprio»

Associazioni criminali specializzate e composte da diverse professionalità

Grazie per l'attenzione!

FORENSICA

Barbara.indovina@forensica.guru

@barbaraindovina

HACK IN BO
Winter 2020 Edition
15ª EDIZIONE