DEFENSIS

MILANO, 7 MAGGIO 2019

TECNOLOGIA, LAVORO E CONTENZIOSO

«faccio molti più danni io con un mio portatile in pigiama seduto di fronte alla prima tazza di Earl Grey di quanti ne faccia tu in un anno sul campo»

DEFENSIS

Scenario tecnico/legale

- La normativa **abbandona le prescrizioni** minime (GDPR,NIST, AGID…)
- E’ l’azienda che **sceglie misure adeguate** per proteggere il patrimonio aziendale
- Obbliga alla **notifica** / whistleblowing
- **Capacità degli hacker** di mirare e **aspettare** (I collaboratori non ne hanno bisogno)

DEFENSIS

Momento del rapporto di lavoro

4) Policy sull'utilizzo degli strumenti aziendali

1) Indagini pre-assunzionali

2) Monitoraggio delle attività svolte

5) Investigazioni

2) Perizie Informatiche

DEFENSIS

PRE-EMPLOYMENT SCREENING / VERIFICA PREASSUNTIVA

TERMS & CONDITIONS RELATING TO THE PRE-EMPLOYMENT SCREENING PROCESS (ENG)

By signing this document, I explicitly authorize _____ (hereafter "the Company") to carry out specific pre--employment screening as indicated in this document. The pre--employment screenings are to verify (depending upon the role which I am applying for with the Company, and its seniority and sensitivity) my identity, qualifications, work experience, my ability to work with the Company in the country concerned, and that there are no important relevant factors concerning me which would lead the Company not to hire me in view of the position for which I apply.

Types of Personal Information Collected
For the purposes of pre--employment verifications, the personal information that is collected about me is provided by me on forms relating to my prospective employment with the Company. Some specific examples of this information are (i) identification and address information, (ii) education and qualifications, (iii) past employment and positions held in other organizations, (iv) professional qualifications and registrations with professional bodies, and (v) criminal convictions, and may also include (vi) financial information.

Use of My Personal Information
The Company will need to use, disclose, and transfer the

CONDIZIONI RELATIVE ALLA VERIFICA PREASSUNTIVA (ITA)

Firmando questo documento autorizzo esplicitamente _____ (qui di seguito, « la Società ») a intraprendere la verifica preassuntiva indicata nel presente documento. Le verifiche preassuntive hanno la funzione di verificare (a seconda del ruolo per il quale mi candido presso la Società, nonché alla sua posizione gerarchica e al suo grado di sensibilità) la mia identità, le mie qualifiche, la mia esperienza lavorativa, la mia capacità di lavorare presso la Società nel paese in questione, e che non vi siano fattori importanti a me relativi che potrebbero portare la Società a non assumermi in considerazione della posizione alla quale mi candido.

Tipi di informazioni personali raccolte
Ai fini delle verifiche preassuntive, le informazioni personali raccolte su di me sono quelle da me fornite sui moduli di candidatura per un'eventuale assunzione da parte della Società. Alcuni esempi specifici di tali informazioni sono (i) informazioni di identificazione e relative al mio indirizzo, (ii) istruzione e qualifiche, (iii) impieghi passati e posizioni ricoperte in altre organizzazioni, (iv) qualifiche professionali e iscrizioni a organi professionali e (v) condanne penali, e potrebbero includere anche (vi) informazioni finanziarie.

Uso dei miei dati personali
La Società avrà bisogno di usare, comunicare e trasferire le

DEFENSIS

CONCORRENZA SLEALE, FURTO, DATA LEAK…

Abbiamo informazioni sufficienti?

DEFENSIS

Aveva dei beni aziendali in uso?

DEFENSIS

Abbiamo informazioni sufficienti?

ALTRA ATTIVITA' IN ORARIO D'UFFICIO

E' **previsto** che venga raccolto quel tipo di dato?

DEFENSIS

Abbiamo informazioni sufficienti?

FURTO DI INFORMAZIONI

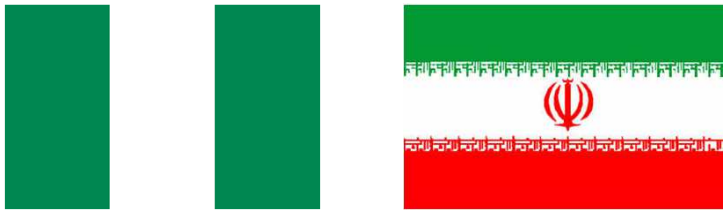
Le informazioni digitali **cancellate** possono essere irrecuperabili

Il dispositivo su cui è transitato il dato **non c'è più**

DEFENSIS

Abbiamo informazioni sufficienti?

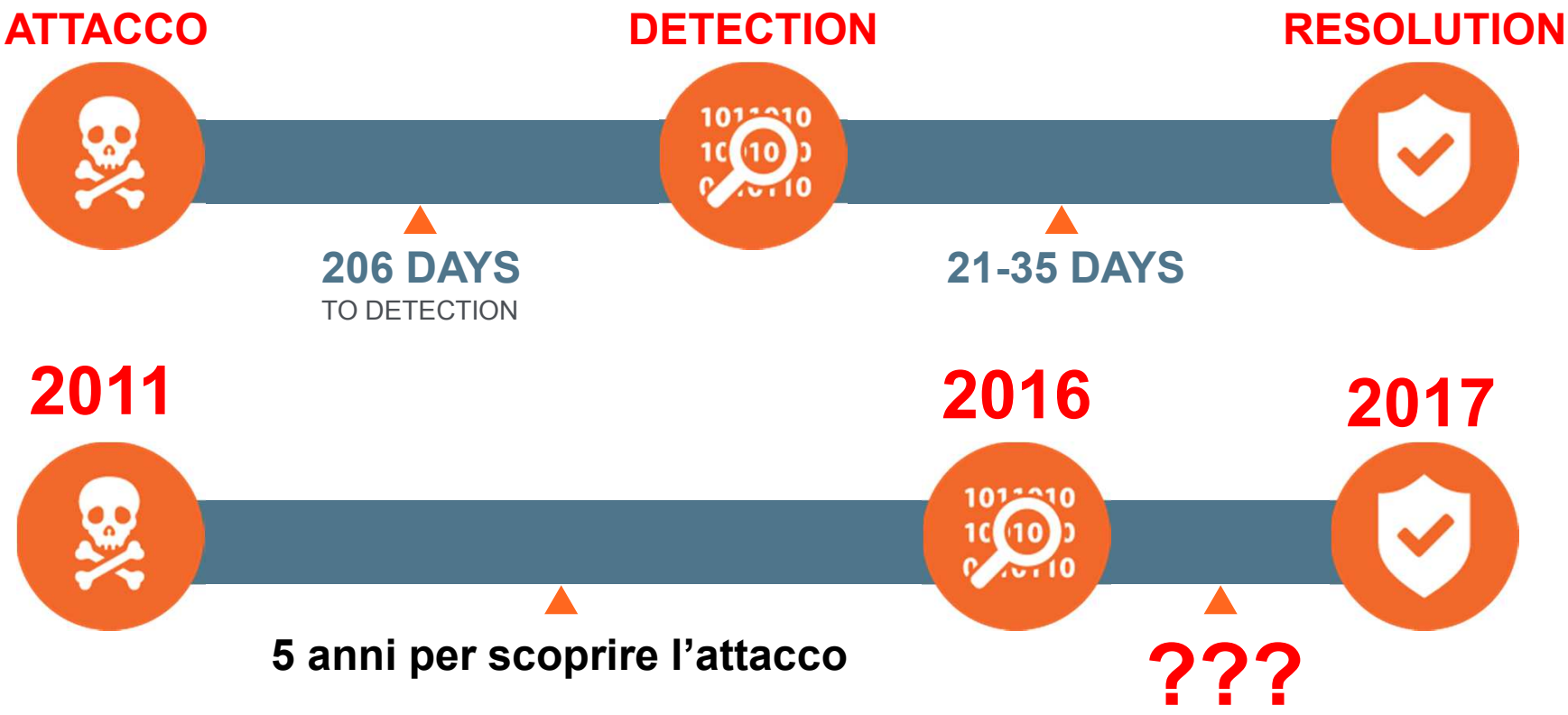
FURTO IDENTITA' e HACKING



E' **previsto** che venga raccolto quel tipo di dato?

Qualcuno verifica la sicurezza di server/applicazioni in «**cloud**»?

DEFENSIS


ATTACCO
DETECTION
RESOLUTION
206 DAYS
TO DETECTION
21-35 DAYS
2011
2016
2017
5 anni per scoprire l'attacco
???

DEFENSIS

L'articolo 23 del D.Lgs 151/2015 attuativo del Jobs Act è diventato il punto di riferimento normativo per quanto concerne la tutela del patrimonio aziendale.

I dati raccolti dagli strumenti di lavoro aziendali possono essere utilizzati «a tutti i fini connessi al rapporto di lavoro, a condizione che:

- Definizione di strumento aziendale
- Adeguata informazione
- Non eccedenza nel controllo
- Precisa informazione su modalità e descrizione dei controlli effettuati
- Security by design nel trattamento del dato (GDPR 2018)

DEFENSIS

14.3 Nella gestione dei sistemi informatici aziendali, e degli strumenti di lavoro, il servizio ICT, o **terzi** incaricati dalla direzione, potranno acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali: i log generati da Microsoft Windows/Android/iOS, gli accessi alla rete e ai dispositivi aziendali, la cancellazione, creazione o esportazione/trasferimento di file e informazioni, l'uso di file/software di carattere non lavorativo. I dati verranno conservati per **206 giorni** e quindi cancellati. Tali informazioni potranno essere utilizzate in caso di attacco informatico, incidente informatico e ai sensi del successivo punto X, **per tutti i fini connessi al rapporto di lavoro**, sempre nell'ambito delle finalità individuate nel precedente punto Y, e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

DEFENSIS

Si sono dovuti notificare 18.478 clienti che le loro informazioni personali sono state diffuse a seguito della **violazione dell'account email** di un dipendente.

#notifica #reputazione #formazione

www.defensis.it/risorse-eventi/account_check.html

DEFENSIS

24.000 clienti coinvolti nella perdita di informazioni dovuta al **furto** di un **PC**.

#sicurezzafisica #procedure

DEFENSIS

I dati medici di 29.000 pazienti sono stati **impropriamente trattati** da parte di un dipendente del call center esterno.

#censimento #permessi

DEFENSIS

Notifica a 5.300 clienti che I loro dati sono stati disponibili online per due anni a causa di una **applicazione web non sicura**.

#vulnerability_assessment #forensic_readiness

GRAZIE

MICHELE COGO
michele.cogo@defensis.it