PRIVACY: ULTIMA FRONTIERA?

CYBER SECURITY NATIONAL LAB – UNIPG

CYBERSECURITY DAY 2018 – 9 OTTOBRE 2018

UNIVERSITÀ DEGLI STUDI DI PERUGIA

AVV. FILIPPO BIANCHINI

PRIVACY VS. DATA PROTECTION

Thanks to Giovanni Ziccardi

Il modello americano di **privacy** inteso come «*right to be let alone*»

(v. Samuel Warren e Louis Brandeis, "**The Right to Privacy**", Harvard Law Review, 1890)

approda in Europa, dove diventa **data protection**

(protezione dei dati dei cittadini rispetto a chi li tratta in maniera automatizzata, v. schedatura FIAT)

Transatlantic divide

TASSONOMIA DELLA PRIVACY

Rachel L. Finn et al.,
Seven types of privacy

PRIVACY OF PERSON: questa categoria è focalizzata sul corpo di una persona ed il diritto di essere liberi da qualsiasi invasione non autorizzata (art. 13 Cost.)

- Uso di chip di identificazione a radiofrequenza (RFID) impiantati per autorizzazione attraverso porte di sicurezza, autenticazione ai sistemi o accesso all'hardware di calcolo e dati biometrici • Test genetici, test antidroga o informazioni sugli interventi chirurgici • Dispositivi di scansione passeggeri negli aeroporti

PRIVACY OF BEHAVIOUR AND ACTION: questa categoria è un'estensione della precedente ed è focalizzata su pensieri ed emozioni prima che siano espressi a qualcuno, attività nello spazio pubblico e privato e monitoraggio mirato. Comprende le questioni relative alle attività personali, gli orientamenti e le preferenze che sono di natura sensibile e potrebbero determinare impatti sugli individui associati (artt. 16 e 21 Cost.)

- Uso di telecamere per catturare i conducenti che commettono violazioni del codice stradale • Uso di *body-worn camera*

PRIVACY OF COMMUNICATION: questa categoria concerne la protezione dei modi in cui le persone comunicano con gli altri utilizzando qualsiasi tipo di mezzo di comunicazione (stampato, vocale, visivo e digitale) (art. 15 Cost.)

- Uso di strumenti di intercettazione delle comunicazioni, quali microfoni nascosti e strumenti che copiano le comunicazioni, come e-mail e messaggi di testo • Un governo che raccoglie informazioni sulle attività dei cittadini senza far loro sapere che tale sorveglianza è in atto

PRIVACY OF DATA AND IMAGE: questa categoria copre la protezione delle informazioni personali in tutte le forme, compresi i dati, le informazioni stampate e le immagini. Le attività all'interno di questa categoria riguardano la definizione di regole che regolano la raccolta, l'uso, la condivisione e la gestione delle informazioni personali.

- Violazione di informazioni finanziarie, informazioni mediche, registri governativi, registrazioni delle attività di una persona su Internet • Foto e video acquisiti e condivisi senza consenso

PRIVACY OF THOUGHTS AND FEELINGS: questa categoria si concentra sulla protezione delle persone per garantire che i loro pensieri e sentimenti non siano condivisi in modo inappropriato con gli altri, o che non siano obbligati a condividere e avere in qualche modo impatti negativi su di loro (artt. 19 e 21 Cost.)

- Essere costretti a fornire password per i social media quando si fa domanda per un posto di lavoro (*)
- Essere costretti a rivelare credenze religiose o opinioni politiche quando si fa domanda per un posto di lavoro

PRIVACY OF LOCATION AND SPACE: questa categoria riguarda il porre limiti alla capacità di intromettersi nella posizione, nello spazio e nell'ambiente generale di un individuo. L'ambiente non è limitato alla casa; include anche il posto di lavoro e gli spazi pubblici. L'invasione nella privacy territoriale di un individuo assume solitamente la forma di monitoraggio (art. 14. Cost.)

- Far volare un drone sopra la proprietà di un individuo per scattare foto
- Registrare individui all'interno della loro proprietà

- (*) In Nuova Zelanda gli agenti alla dogana potranno d'ora in poi effettuare perquisizioni digitali sulle persone chiedendo la password. La nuova legge obbliga i viaggiatori a fornire l'accesso ai loro apparecchi – quindi impronta o password – se gli agenti hanno un ragionevole sospetto di qualche reato. Qualora si rifiuti di dare la password multa fino a 5mila dollari e telefono sequestrato e sottoposto ad analisi forense.

  (da «Guerre di Rete», newsletter a cura di Carola Frediani, numero 6)

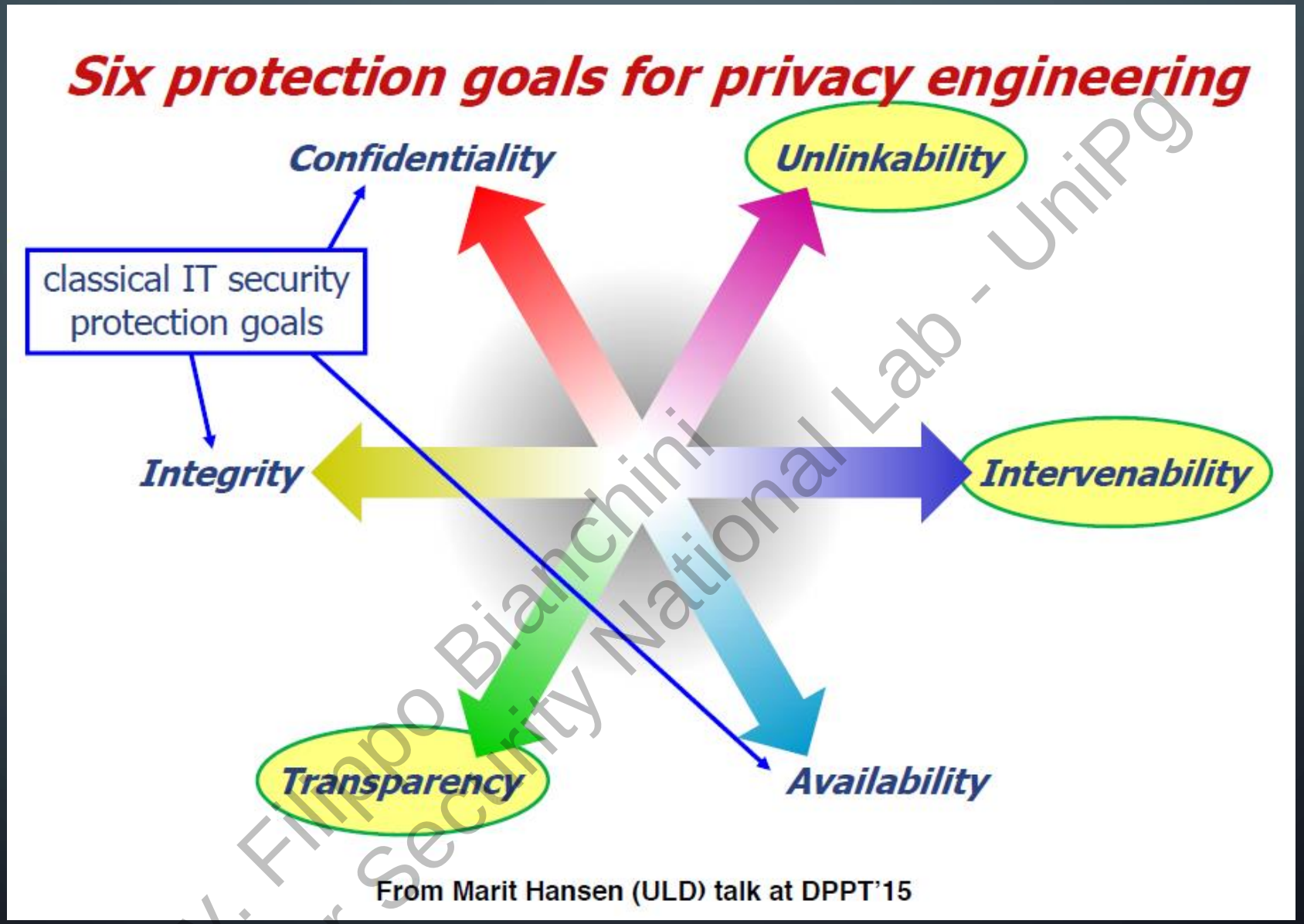
PRIVACY OF ASSOCIATION: questa categoria riguarda il diritto delle persone ad associarsi con chiunque vogliano, senza monitoraggio o emarginazione non autorizzati (artt. 17 e 18 Cost.).

- Test del DNA che dimostrino l'etnia • Datori di lavoro che usano il test del DNA per prendere decisioni • Qualsiasi tipo di segregazione basata su religione, comportamento, assemblea o appartenenza

RISCHI PER LA PRIVACY NEL CYBERSPAZIO

Minacce	Vulnerabilità	Rischi
- Dispositivi potenti e portatili (ad esempio smartphone, tablet e laptop) che facilitano sempre più la raccolta, l'aggregazione e la diffusione delle informazioni - Aumento del numero di relazioni con terze parti (ad esempio, fornitori di connessione e applicazioni) - Aumento della concentrazione dell'infrastruttura del cyberspazio (ad es. datacenter e dorsali di comunicazione) - Leggi e regolamenti che compromettono la privacy - Professionalità degli aggressori (ad esempio, singoli cracker e team finanziati da Stati)	- Crescente numero di persone operanti nel cyberspazio - Aumento del numero di fonti per la raccolta di dati (ad es. telecamere, dati biometrici, GPS, RFID, ecc.) - Utenti non istruiti / inconsapevoli in materia di privacy del cyberspazio - Mancanza di consapevolezza in ordine ai problemi di protezione della privacy nello sviluppo di applicazioni / sistemi - Maggior quantità di dati memorizzati elettronicamente ed elaborati su scala massiccia e centralizzata (ad esempio, data warehouse) - Informazioni condivise, combinate e collegate insieme con maggiore frequenza - Utilizzo di credenziali comuni per accedere a più sistemi	- Raccolta di informazioni non necessarie allo scopo - Mantenimento delle informazioni oltre il tempo di conservazione - Divulgazione di informazioni sensibili sulla propria vita o attività - Circolazione di informazioni errate che compromettono la reputazione - Furto di identità - Applicazioni / sistemi privi di funzionalità / controlli di protezione della privacy adeguati

- Attenzione: poiché il valore delle informazioni dipende molto dal contesto in cui viene valutato, alcune informazioni considerate innocue, se combinate o aggregate con altre informazioni, possono dare origine a informazioni con un potenziale di danno elevato.



RELAZIONI TRA SECURITY E PRIVACY

Thanks to Claudio Bettini

Security principles	*Privacy principles*
CONFIDENTIALITY: only authorized parties can access data authentication (encryption of data in transfer, at rest, and in use)	**TRANSPARENCY**: all privacy-relevant data processing (legal, technical, organisational) can be understood and reconstructed at any time
INTEGRETY: data should not be altered without authorization (hashing, checksums)	**UNLINKABILITY**: privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context. More specifically it includes de-identification, pseudonimization, generalization, data minimization, separation
AVAILABILITY: whenever needed, the system should be available (replication, backup, …)	**INTERVENABILITY**: intervention is possible concerning all ongoing or planned privacy-relevant data processing

SICUREZZA DEL TRATTAMENTO (ART. 32, PAR. 1, GDPR)

- «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate** per garantire un **livello di sicurezza adeguato al rischio** […]» (cfr. Cons. 83)

MISURE TECNICHE E ORGANIZZATIVE (ESEMPI)

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personale in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

RISK-BASED APPROACH (ART. 32, PAR. 2, GDPR)

- «Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei **rischi** presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati»
- Per «rischio» si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità» per i diritti e le libertà (WP29 248)

ERRORI DA EVITARE

Non bisogna confondere la gestione dei rischi con il tema delle misure di sicurezza

Il rischio non si riferisce al titolare, ma al soggetto interessato

DALLA *SECURITY BY DESIGN...*

Open Web Application Security Project (OWASP) Developer Guide

Ridurre al minimo la superficie di attacco	• Every feature that is added to an application adds a certain amount of risk to the overall application. The aim for secure development is to reduce the overall risk by reducing the attack surface area.
Stabilire impostazioni predefinite sicure	• There are many ways to deliver an "out of the box" experience for users. However, by default, the experience should be secure, and it should be up to the user to reduce their security – if they are allowed.
Principio del minimo privilegio	• The principle of least privilege recommends that accounts have the least amount of privilege required to perform their business processes. This encompasses user rights, resource permissions such as CPU limits, memory, network, and file system permissions.
Principio della difesa in profondità	• The principle of defense in depth suggests that where one control would be reasonable, more controls that approach risks in different fashions are better. Controls, when used in depth, can make severe vulnerabilities extraordinarily difficult to exploit and thus unlikely to occur.

Fallire in sicurezza	• Applications regularly fail to process transactions for many reasons. How they fail can determine if an application is secure or not.
Non fidarsi dei servizi di terze parti	• Many organizations utilize the processing capabilities of third party partners, who more than likely have differing security policies and posture than you. It is unlikely that you can influence or control any external third party, whether they are home users or major suppliers or partners.
Separazione dei doveri	• A key fraud control is separation of duties. For example, someone who requests a computer cannot also sign for it, nor should they directly receive the computer. This prevents the user from requesting many computers, and claiming they never arrived.
Evitare la *security through obscurity* – Legge di Linus	• Security through obscurity is a weak security control, and nearly always fails when it is the only control. This is not to say that keeping secrets is a bad idea, it simply means that the security of key systems should not be reliant upon keeping details hidden. • *Given enough eyeballs, all bugs are shallow.*

Mantenere la sicurezza semplice

- Attack surface area and simplicity go hand in hand. Certain software engineering fads prefer overly complex approaches to what would otherwise be relatively straightforward and simple code.

Risolvere correttamente i problemi di sicurezza

- Once a security issue has been identified, it is important to develop a test for it, and to understand the root cause of the issue. When design patterns are used, it is likely that the security issue is widespread amongst all code bases, so developing the right fix without introducing regressions is essential.

… ALLA *PRIVACY BY DESIGN*

Thanks to Nicola Fabiano

- A metà degli anni '90, a livello internazionale, si è sottolineato il notevole cambiamento riguardante la privacy, che ha delineato delle nuove direttive riguardo alle cosiddette *PET* (*Privacy Enhancing Technologies*), ossia tutte quelle tecnologie nell'ambito dell'ICT utili ad accrescere la protezione dei propri dati personali.
- Nel 2010 la 32a Conferenza mondiale dei Garanti privacy ha adottato la risoluzione sulla Privacy by Design (PbD) rendendo in tal modo ufficiale questo nuovo concetto che era comunque già noto ed utilizzato negli Stati Uniti e in Canada ← la descrizione ben definita della Privacy by Design è stata elaborata dalla dott.ssa **Ann Cavoukian**, membro della Information and Privacy Commissioner of Ontario, Canada. Secondo la dott.ssa Cavoukian, l'utente è considerato il centro del sistema privacy (per definizione, quindi, è *user centric*).

Privacy by Design

Positive Sum

By Default

Embedded

Proactive/Preventative

Lifecycle Protection

Respect for Users

Visibility/Transparency

AVV. FILIPPO BIANCHINI

LA PbD COMPRENDE A) UNA TRILOGIA DI APPLICAZIONI

Sistemi IT	Pratiche commerciali corrette	Progettazione strutturale e infrastrutture di rete

B) 7 PRINCIPI DEFINITI «FONDAZIONI»

Proattivo non reattivo – prevenire non correggere	• L'approccio alla privacy deve essere di tipo proattivo piuttosto che reattivo; l'obiettivo è quello di anticipare gli eventi e non attendere che essi si verifichino per proporre rimedi alle soluzioni.
Privacy come impostazione di default	• Si intende realizzare il massimo livello di privacy assicurando che i dati personali siano automaticamente protetti in un qualunque sistema IT o commerciale. Non deve essere richiesta alcuna azione specifica da parte dell'individuo per proteggere la propria privacy.
Privacy incorporata nella progettazione	• La privacy deve essere incorporata nell'architettura dei sistema e delle pratiche commerciali e non costituire un *quid pluris*, un elemento da apporre successivamente.

Massima funzionalità – Valore positivo, non valore zero	• L'obiettivo è quello di bilanciare le diverse esigenze ed i diversi obiettivi, con un approccio "*win-win*", evitando compromessi non necessari ed il pretesto di false dicotomie come *privacy vs. security*, dimostrando che è possibile traguardare entrambe.
Sicurezza fino alla fine – Piena protezione del ciclo vitale	• Le misure di sicurezza essenziali per la privacy devono essere applicate durante l'intero ciclo di vita dei dati, dall'acquisizione alla dismissione (Data Governance).
Visibilità e trasparenza – Mantenere la trasparenza	• Tutti i soggetti interessati, indipendentemente dalla prassi aziendale o dalla tecnologia, devono poter effettuare in qualsiasi momento verifiche sui propri dati in assoluta trasparenza.

SOPRATTUTTO…

Rispetto per la privacy dell'utente – Centralità dell'utente

- PbD richiede di porre al primo posto gli interessi dell'individuo, adottando misure quali una privacy robusta di default, opportune notifiche e opzioni *user-friendly*, con un approccio *user-centric*

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE *PRIVACY BY DESIGN* (ART. 25, PAR. 1, GDPR)

Tenendo conto dello **stato dell'arte** e dei **costi di attuazione**, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, **sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso**

il titolare del trattamento mette in **atto misure tecniche e organizzative adeguate**, quali la pseudonimizzazione, volte

ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione e

a integrare nel trattamento le necessarie garanzie

al fine di **soddisfare i requisiti del presente regolamento** e tutelare i diritti degli interessati.

PROTEZIONE PER IMPOSTAZIONE PREDEFINITA *PRIVACY BY DEFAULT* (ART. 25, PAR. 2, GDPR)

- «Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica».

IMPLEMENTAZIONE LA CYBER SECURITY A SUPPORTO DELLA PRIVACY

OBIETTIVI

- **Autonomia personale**: una persona dovrebbe essere in grado di fare le proprie scelte e non essere soggetta a decisioni arbitrarie.
- **Autovalutazione e processo decisionale**: a una persona dovrebbero essere fornite informazioni e conoscenze sufficienti, pertinenti e appropriate per valutare quando è opportuno rinunciare ad alcuni aspetti della privacy.
- **Necessità di comunicazioni limitate e protette**: una persona necessità opportunità per condividere informazioni confidenziali con altre persone di sua scelta.

IN TERMINI PRATICI…

Questi obiettivi possono essere soddisfatti mediante:

- definizione esplicita delle esigenze e aspettative della privacy;
- sviluppo di applicazioni e sistemi basati su requisiti e framework solidi;
- istruzione, formazione e consapevolezza delle persone riguardo agli aspetti della privacy nel cyberspazio.

BUONE PRATICHE PER GLI INDIVIDUI

Verifica le politiche sulla privacy

- Se un'organizzazione non ha una politica esplicita relativa alla protezione delle informazioni personali, non è un buon segno di come gestiscono le informazioni sensibili. Questa stessa regola è applicabile alle app installate sui tuoi dispositivi.

Pensa prima di postare

- Nei social network, nei forum e nelle chat, pubblica solo le informazioni strettamente necessarie, perché i motori di ricerca possono correlare e aggregare post, messaggi e profili casuali e ottenere informazioni che non vuoi che siano.

Fai uso dell'anonimato

- Quando non è essenziale per l'utente identificare le informazioni sensibili, utilizzare le credenziali senza informazioni identificabili personalmente o soluzioni per navigare in modo anonimo, come TOR.

Proteggi il tuo dispositivo e le tue comunicazioni

- Assicurati di installare e mantenere sul tuo dispositivo firewall, crittografici (ad es., Veracrypt e VPN) e soluzioni anti-malware. Il primo impedisce che il tuo dispositivo venga violato e da attacchi remoti, il secondo aiuta a proteggere i dati e i dati memorizzati in transito e l'ultimo può impedire l'uso di malware per tracciare le tue abitudini di navigazione. Per impedirne l'accesso diretto (in caso di furto), assicurarsi di impostare i passcode per accedervi ogni volta che vengono utilizzati. E, infine, evitare a tutti i costi di far uso di Wi-Fi aperte e, se è necessario utilizzarle, non inviare informazioni sensibili.

Utilizza soluzioni crittografiche nel cloud

- Oggi è quasi normale che i servizi cloud crittografino i dati degli utenti per impedire l'accesso non autorizzato. Anche così, prendi in considerazione l'idea di aggiungere le tue soluzioni crittografiche (invia i tuoi dati al cloud già crittografati).

Imposta il software per la privacy

- Assicurati di configurare le opzioni di privacy disponibili nel software che utilizzi. «Non tracciarmi» e «elimina la cronologia dopo la disconnessione» sono alcune opzioni che puoi trovare.

Usa le tue password con saggezza

- Usa password diverse tra tutti i servizi a cui ti unisci, specialmente quelli che usi per siti crittografati o sicuri. Pensa all'utilizzo del software password vault, che genera e memorizza password solide e univoche e autenticazione a due fattori ogni volta che è disponibile.

Segui il tuo istinto

- Se ti senti a disagio a divulgare informazioni, o pensi che le informazioni richieste siano troppo invadenti, personali o irrilevanti per il servizio o il contenuto che stai cercando di ottenere, non farlo.

BUONE PRATICHE PER LE ORGANIZZAZIONI

Avere (e seguire) una politica sulla privacy

- Un'organizzazione dovrebbe avere linee guida chiare per i suoi utenti e dipendenti su quali informazioni vengono raccolte, per quale scopo, come viene utilizzato, per quanto tempo è conservato e come è protetto. Nota che queste linee guida devono essere conformi alle leggi e ai regolamenti locali, quindi dovrai mappare anche questi requisiti legali.

Sapere cosa si ha

- Un inventario di dati dovrebbe essere disponibile per comunicare a un'organizzazione tutte le informazioni personali che ha sugli utenti, chi ne è responsabile e chi può accedervi.

Includere i requisiti di privacy nel processo di sviluppo di applicazioni / sistemi

- Requisiti semplici come la PbD, l'accesso degli utenti con privilegi minimi, la privacy come impostazione predefinita e la sicurezza end-to-end (ad es. da utente a database) possono essere sufficiente per architetti software, sviluppatori e programmatori per comprendere che i problemi di privacy devono essere una parte essenziale dello sviluppo e della manutenzione di applicazioni / sistemi.

Applicare le politiche

- Non basta avere in atto una politica perché tutti la seguano. Pertanto, quando possibile, occorre assicurarsi che seguire la politica sia l'unico modo per utilizzare il sistema. Ad esempio, se il sistema stabilisce che la lunghezza minima della password è di otto caratteri, non deve poter essere per un utente impostarne una più breve.

Fornire mezzi per educare gli utenti

- Le pagine sulla privacy, le newsletter, la formazione video e altre forme di educazione devono essere considerate per rendere gli utenti (ad esempio, clienti, dipendenti, terzi, ecc.) consapevoli di cosa dovrebbero fare per proteggere la loro privacy e quella altrui.

Mantenere l'infrastruttura snella ed aggiornata

- Disporre solo delle risorse minime necessarie per gestire il business e aggiornare le patch di sicurezza ridurrà al minimo la superficie di attacco che qualcuno può utilizzare per compromettere la privacy degli utenti.

Controllo delle modifiche

- L’accesso alle risorse nuove o aggiornate può compromettere tutte le attività di sicurezza. Assicurarsi che i cambiamenti nell'ambiente tecnologico non influenzino i tuoi livelli di sicurezza.

Proteggere la rete e le comunicazioni

- Assicurarsi che i dati degli utenti siano al sicuro durante il trasporto (ad es. tramite VPN, SSL, HTTPS, ecc.). Anche le reti e le comunicazioni interne dell'organizzazione dovrebbero prendere in considerazione misure di protezione.

Prepararsi per le violazioni dei dati

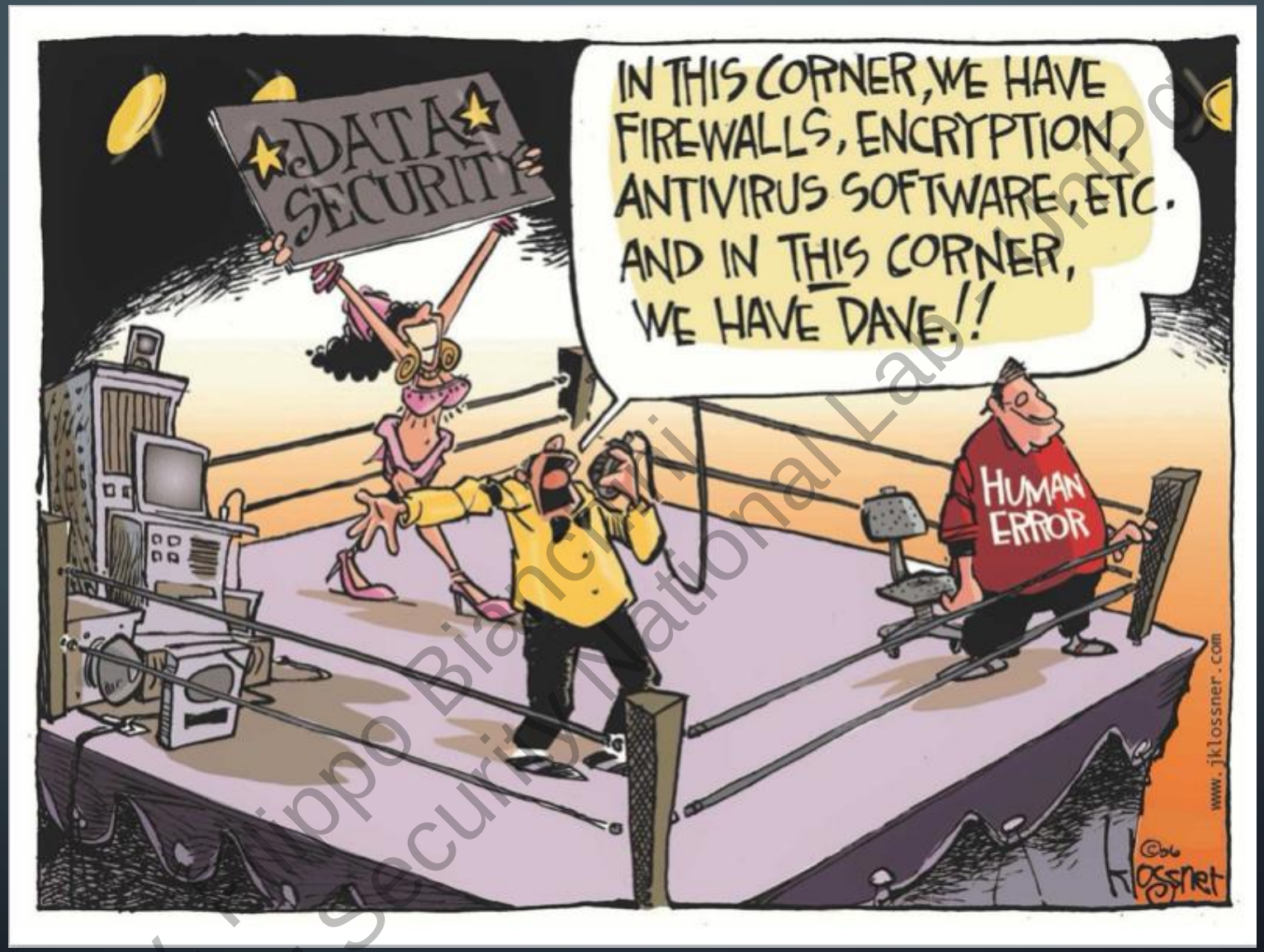
- Questi tipi di incidenti sono inevitabili e occorre essere pronti a rispondere nel modo più rapido ed efficace. Una buona risposta non solo minimizza il danno alla fiducia per gli utenti, ma può minimizzare anche i rischi legali mostrando la dovuta cura nell'organizzazione dei dati «sensibili».

Valutazione periodica:

- Mediante audit, *vulnerability assessment* e *penetration test*, un'organizzazione può valutare (e far valutare) l'efficacia dei propri controlli di sicurezza ed apportare, quindi, le opportune modifiche per mantenere i livelli di sicurezza. Anche la simulazione di *data breaches* dovrebbe essere presa in considerazione per valutare la performance dei piani di risposta.

Fornire un canale di comunicazione:

- Gli utenti non vogliono solo essere informati su ciò che un'organizzazione si propone di proteggere i propri dati, ma vogliono anche porre domande ed avere riscontro ai reclami. Rendendo disponibili una pagina, un numero di telefono, un'e-mail o altre forme di comunicazione e rispondendo agli input degli utenti, un'organizzazione può migliorare la propria immagine come un detentore affidabile di dati / informazioni.



GRAZIE PER L'ATTENZIONE

AVV. FILIPPO BIANCHINI

DPO UNI 11697:2017

UNIDPO
Unione Nazionale Italiana Data Protection Officer

avv.filippobianchini@gmail.com –
info@studiolegalebianchini.eu

@legale

iustec

studiolegale