LPD

ellepidi.ch

Mattia Munari

Senior System Engineer

mattia@informatich.ch

+41 91 601 40 60

www.linkedin.com/in/mattia-munari/

Programma

- introduzione;
- registro dei trattamenti;
- anonimizzazione dei dati; (ospite dott. Gianluca Gilardi)
- misure minime;
- domande e risposte.

InformatiCH Sagl

- nasce nel 2018 dal consolidamento di realtà precedenti;
- offre progettazione, consulenza e assistenza in campo informatico;
- gestisce progetti ad Hoc su richiesta del cliente;
- servizi di sicurezza informatica: assessment, pt, normativa, post-incident response;
- servizi Legal Tech.

Chi siamo

- nel 2020 inizia la collaborazione con Angela Pedàlina per i servizi Legal Tech;
- nel 2021 si delineano gli ultimi dettagli sulla legge LPD;
- e quindi…

Legal

Tech

Premessa

I dati sono diventati il nuovo petrolio.

IoT, controlli biometrici, riconoscimento facciale, tracciamento di persone, dispositivi connessi, ecc…

Perché la protezione dati personali è importante?

Perché giornalmente noi in maniera più o meno consapevole diffondiamo dati. Lo facciamo quando ad es. navighiamo su un sito Internet alla ricerca di un prodotto o di un servizio, e quindi comunichiamo quelle che sono le nostre preferenze; lo facciamo quando ecc...

Cosa mai potrà andare storto?

Quindi in tutti questi casi **vengono usati dati personali** e l'obiettivo della nuova legge è proprio la difesa dei diritti del singolo per quanto riguarda il trattamento di tutte queste informazioni; per la legge ogni persona deve essere in grado accettare liberamente, quali informazioni, quali dati personali che la riguardano possono essere trasmessi quando, dove e naturalmente a chi. Inoltre vuole **responsabilizzare** chi fa uso di questi dati **per motivi professionali**.

I rischi

Aprile 2021

Databreach Facebook:

- +500M persone coinvolte:
- nome completo, numero di telefono, localizzazione, indirizzI e-mail e informazioni anagrafiche;
- possono essere usati per impersonare le Persone Interessate per commettere frodi.
- Facebook si rifiuta di avvisare le singole persone.

Aprile 2021

Databreach LinkedIn:

- +500M di persone coinvolte;
- nome completo, indicazione di genere, indirizzo email, numeri di telefono, link ad account social media, informazioni del posto di lavoro.
- Microsoft sostiene che siano state carpite solo informazioni pubblicamente disponibili dalla piattaforma.

Angela Pedàlina

Giurista

angela@informatich.ch

+41 91 601 40 60

www.linkedin.com/in/angela-pedalina

Alcune indicazioni sulla Legge Federale

- 25 Settembre 2020
- Persone Fisiche
- Obblighi del Titolare del Trattamento

Registro dei Trattamenti : considerazioni

- accountability, responsabilizzazione del Titolare del Trattamento;
- biunivoca funzione del Registro dei Trattamenti;
- informazioni aggiuntive; (valutazione impatto e quali sono stati i risultati, quali sono i luoghi in cui si conservano i dati)
- costante aggiornamento.

Art. 12 Legge Protezione dei Dati

I **Titolari** e i **Responsabili** del trattamento tengono **ognuno** un registro delle rispettive **attività di trattamento**.

Il registro del Titolare del trattamento contiene almeno:

a. l'**identità** del Titolare del trattamento;
b. lo **scopo** del trattamento;
c. una **descrizione** delle categorie delle persone interessate e delle categorie di dati personali trattatati;
d. le **categorie** di destinatari;
e. se possibile, la **durata** di **conservazione** dei dati personali o i criteri per determinare tale durata;
f. se possibile, una descrizione generale dei **provvedimenti** tesi a garantire la sicurezza dei dati personali secondo l'art. 8;
g. se i dati personali sono comunicati all'**estero**, le indicazioni relative allo **stato destinatario** e le rispettive **garanzie**.

Art. 30 GDPR

Chi deve predisporre il Registro dei Trattamenti secondo la LPD?

→ **Tutte** le aziende che hanno più di 250 collaboratori;

→ Aziende con meno di 250 collaboratori che hanno dei trattamenti con **rischio medio – alto**.

Si suggerisce a tutte le aziende di istituire un Registro dei Trattamenti.

Il Registro dei Trattamenti è un documento che deve contenere le informazioni sui trattamenti che vengono svolti.

MAPPATURA DATI

- La prima cosa che si deve fare per capire quali sono gli adempimenti da mettere in atto per adeguarsi alla LPD è una MAPPATURA.

Quali dati si stanno raccogliendo?

- Avvocato – Dati anagrafici dei clienti per la fatturazione, dati relativi allo stato civile, alla situazione economica, al patrimonio, ai figli (quindi anche dati di minori), alle abitudini di vita;
- Medico – Dati anagrafici dei clienti per la fatturazione, dati relativi alla storia clinica del paziente, eventuali familiarità con patologie diverse, dati che riguardano persone all'interno del suo nucleo familiare;

ELENCO DEI TRATTAMENTI

Una volta raccolti questi dati si avranno tutti i tipi di Interessati (i soggetti dei quali si stanno trattando i dati), si avranno tutti i tipi di Dati che si trattano e si avrà un elenco dei Trattamenti che si effettuano.

Sono Trattamenti : la raccolta, la registrazione, la suddivisione in categorie, la modifica, l'estrazione, la consultazione, l'uso, la diffusione o la comunicazione a soggetti terzi ed infine la cancellazione.

Tutto ciò è necessario per la creazione del primo documento compliance della propria realtà aziendale alla LPD.

Al Titolare del Trattamento deve quindi essere chiaro tutto il flusso dei dati

- Che tipo di dati si raccoglie, da chi, come li si ottiene, quali operazioni vengono svolte su questi dati, chi è autorizzato a vederli (collaboratori), se il trattamento è telematico o cartaceo e i tempi di conservazione – cancellazione

Esempio LovePharma Sa

Registro dei trattamenti

Dati organizzazione

Nome dell'organizzazione	**LovePharma Sa**
Indirizzo	Corso Elvezia 1, Chiasso

Titolare

Nome dell'organizzazione	**LovePharma Sa**

Consulente della protezione dei dati

Nome e Cognome (facoltativo)	**Loris Bernasconi**

Descrizione attività

LovePharma Sa si occupa di sviluppare e commercializzare prodotti farmaceutici.

Esempio LovePharma Sa

Trattamenti

- Interni:
  - trattamento di dati personali di dipendenti e collaboratori;
  - trattamento di dati personali di candidati;
  - trattamento di dati personali di clienti e fornitori;
  - trattamento di dati personali di visitatori e ispettori;
  - trattamento di dati personali per newsletter;
  - trattamento di dati personali nei servizi TIC.
- Esterni:
  - registrazione pagamenti o salari affidati al fiduciario;
  - videosorveglianza;
  - dati personali nello svolgimento delle attività commerciali.

Informazioni aggiuntive

  - valutazione di impatto: esito;
  - luoghi in cui vengono conservati i dati.

Esempio LovePharma Sa

Trattamento di dati personali di candidati

- Data prima redazione: **28.03.19**
- Data ultimo aggiornamento: **20.06.21**

Trattamento

Dati personali di candidature spontanee

Finalità del trattamento

L'organizzazione tratta dati personali di persone esterne che si candidano a posizioni interne allo scopo di essere assunti o di essere impiegati per le seguenti finalità:

- Consultazione del cv
- Valutazione delle competenze
- Protezione dei sistemi informatici

Persone interessate

Candidati, coloro che si candidano per essere impiegati presso l'organizzazione

Categorie di dati trattati

I dati che vengono trattati dalle persone che sottopongono il loro cv alla ns valutazione sono:

- Dati identificativi
- Dati personali degni di particolare protezione

Esempio LovePharma Sa

Categorie di destinatari

Non vi sono altri destinatari ai quali vengono trasmessi alcuni dati

Termini di cancellazione dei dati

- Dati presenti nel cv: 12 mesi
- Dati raccolti dalla rete aziendale: 6 mesi

Contitolari

L'azienda non ha collaborazioni con altre organizzazioni

Misure tecniche organizzative

Segregazione e controllo degli accessi

Comunicazione di dati all'estero e rispettive garanzie

Nessuna comunicazione ad alcuna organizzazione internazionale

Esempio 1

TRATTAMENTO: Gestione paghe	
Titolare trattamento dati	Cognome
	Nome
	E-mail
	N° telefono
Responsabile protezione dati	Cognome
	Nome
	E-mail
	N° telefono
Contitolare	No
Persone autorizzate	No
Sede	
Struttura	Ufficio amministrazione
Soggetti autorizzati	Responsabile amministrazione
PROCESSO DI TRATTAMENTO	
Finalità del trattamento	Compensi, maternità, collaborazioni
Tipo dati personali	Dati anagrafici, codici fiscali
Categorie di interessati	Dipendenti, liberi professionisti, collaboratori, tirocinanti
Categorie di destinatari	Consulente del lavoro
Informativa	Sì

Esempio 2

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*							
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*							
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*							
TIPOLOGIA DI TRATTAMENTO	**FINALITA' E BASI LEGALI DEL TRATTAMENTO**	**CATEGORIE DI INTERSSATI**	**CATEGORIE DI DATI PERSONALI**	**CATEGORIE DI DESTINATARI** *[Indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	**TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI** *[Indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	**TERMINI ULTIMI DI CANCELLAZIONE PREVISTI**	**MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE**

Esempio 3

Trattamenti effettuati in qualità di TITOLARE

Registro dei trattame

Funzione di siness/Unità nizzativa/Dipartimento	Denominazione del trattamento (se individuata)	Finalità del trattamento	Software, Database, Manutenzione	Denominazione e dati di contatto del contitolare (se presente)	Categorie di interessati	Categorie di dati personali	Categorie di destinatar cui i dati sono o posso essere comunicati
lisorse Umane, mministrazione	Pagamento stipendi	Amministrazione del personale	Software XXX in cloud e cartelle su NAS. Manutenzione da remoto	N/A	Dipendenti	Dati relativi alla prestazione lavorativa	Previdenza sociale
Marketing	Marketing diretto	Direct Marketing	Software Fidelity XXX, gestito da agenzia XXX	N/A	Clienti	Dati di identificazione elettronica	Piattaforme di elaborazion

Gianluca Gilardi

LT42 The Legal Tech Company

g.gilardi@lt42.it

+39 02 2111 5050

www.linkedin.com/in/gianluca-gilardi-1519a0b/

L’anonimizzazione nel trattamento dei dati personali

Ovvero: il Santo Graal del Personal Data Processing

La LPD e l’anonimizzazione

«I dati personali sono distrutti o resi anonimi appena non sono più necessari per lo scopo del trattamento.» (art. 6 co. 4 - Principi)

Cosa è “un dato anonimo”?

Il GDPR ci aiuta a dare una (prima) definizione di dato anonimo:
«informazioni che non si riferiscono a una persona fisica identificata o identificabile»

In cosa consiste il processo di anonimizzazione?

L'anonimizzazione è il processo di rimozione degli identificatori personali, **sia diretti che indiretti**, che possono portare all'identificazione di un individuo.

Un individuo può essere identificato **direttamente** dal suo nome, indirizzo, codice postale, numero di telefono, fotografia o immagine, o qualche altra caratteristica personale unica.

Un individuo può essere **indirettamente** identificabile quando alcune informazioni sono collegate con altre fonti di informazione, tra cui il luogo di lavoro, il titolo di lavoro, lo stipendio, il codice postale o anche il fatto che hanno una particolare diagnosi o status.

Ah beh, basta cancellare un po’ di campi dal database, no?

No.

Come ha imparato a sue spese Netflix.

Nel 2008 , NETFLIX ha pubblicato 10 milioni di classifiche di film da parte di 500.000 clienti, come parte di una sfida a proporre sistemi di raccomandazione migliori di quello che la società stava usando. I dati sono stati resi anonimi rimuovendo i dettagli personali e sostituendo i nomi con numeri casuali, per proteggere la privacy dei recensori.
Arvind Narayanan e Vitaly Shmatikov, ricercatori dell'Università del Texas a Austin, hanno de-anonimizzato alcuni dei dati di Netflix confrontando classifiche e timestamp con le informazioni pubbliche dell'Internet Movie Database, o IMDb.

Ah beh, basta cancellare un po’ di campi dal database, no?

“We demonstrate that **an adversary who knows only a little bit about an individual subscriber can easily identify this subscriber’s record in the dataset**. Using the Internet Movie Database as the source of background knowledge, we successfully identified the Netflix records of known users, uncovering their apparent political preferences and other potentially sensitive information.”
(https://arxiv.org/pdf/cs/0610105.pdf)

La sfida dell’anonimizzazione nel contesto dei big data

Il problema dell’anonimizzazione di una base di dati ad alta dimensionalità viene identificato come *NP-hard*, ossia con la caratteristica di essere *almeno* difficile come i più difficili problemi in P/NP. Nella misura in cui ad oggi non è stato possibile identificare un algoritmo efficiente per la soluzione di problemi NP-completi ne consegue che anche per i problemi NP-hard mentre è *teoricamente* possibile che venga elaborato un algoritmo efficiente, allo stato nessun algoritmo del genere è mai stato identificato dalla comunità scientifica, e in generale (pur in assenza di una dimostrazione matematica) si propende per ritenere che un risultato del genere sia **impossibile**.

La pseudonimizzazione NON è anonimizzazione

La "pseudonimizzazione" può essere definita come il trattamento dei dati personali in modo tale in modo tale che i dati personali non possano più essere attribuiti a uno specifico soggetto di dati interessato **senza l'uso di informazioni aggiuntive, a condizione che tali informazioni supplementari siano conservate separatamente e siano soggette a misure tecniche e organizzative per garantire che i dati personali non siano attribuiti a una persona fisica identificata o persona fisica**. Questo significa che l'uso di "informazioni aggiuntive" può portare all'identificazione l'identificazione degli individui, il che è per cui i dati personali pseudonimi sono ancora dati personali. I dati anonimi, invece, non possono essere associati a individui specifici.

La cifratura NON è anonimizzazione

La crittografia non è una tecnica di anonimizzazione, ma può essere un potente strumento di pseudonimizzazione.

Corollario

In un’ottica di minimizzazione del rischio di compliance la cancellazione dei dati è **sempre** l’opzione preferibile.

Non tutto è perduto

In questo momento storico il dibattito è accesissimo relativamente alla possibilità di alimentare sistemi di Machine Learning utilizzando dei dati sintetici che (fatte salve alcune eccezioni mitigabili) si sottraggono all'orbita dei dati personali

Contacts

Unless you happen to have a Bat-Signal at hand...

Innovative? You bet.
Disruptive? No way!

LT42 Srl
VIA VITRUVIO 1
20124 MILANO (MI)
ITALY

OFFICE +39.02.21115050
EMAIL info@lt42.it

Mattia Munari

Senior System Engineer

mattia@informatich.ch

+41 91 601 40 60

www.linkedin.com/in/mattia-munari/

Misure minime e TIC

TIC è l'acronimo italiano di ICT, **Tecnologie dell'Informatica e delle Comunicazioni** (Information and Communication Technology).

Non è semplice dare delle misure minime **universali**, si fa riferimento a normative già attive. Le autorità federali hanno predisposto un documento esplicativo e un foglio excel per effettuare la valutazione e le possibilità di miglioramento.

https://www.bwl.admin.ch/bwl/it/home/themen/ikt/ikt_minimalstandard.html

Percorso di valutazione e miglioramento

Seguendo il materiale proposto dalla Confederazione, si valuta e si interviene secondo diversi temi:

- identificare;
- proteggere;
- intercettare;
- reagire;
- ripristinare.

In tutto vengono proposte una serie di misure concrete, 106 con riferimenti alle norme che le esplicitano.

Riferimenti normativi sulle misure minime

- Legge federale sull'approvvigionamento economico del Paese (Legge sull'approvvigionamento del Paese, LAP; RS 531)
- Ordinanza sull'organizzazione dell'approvvigionamento economico del Paese (RS 531.11)
- Ordinanza sui provvedimenti preparatori in materia di approvvigionamento economico del Paese (RS 531.12)

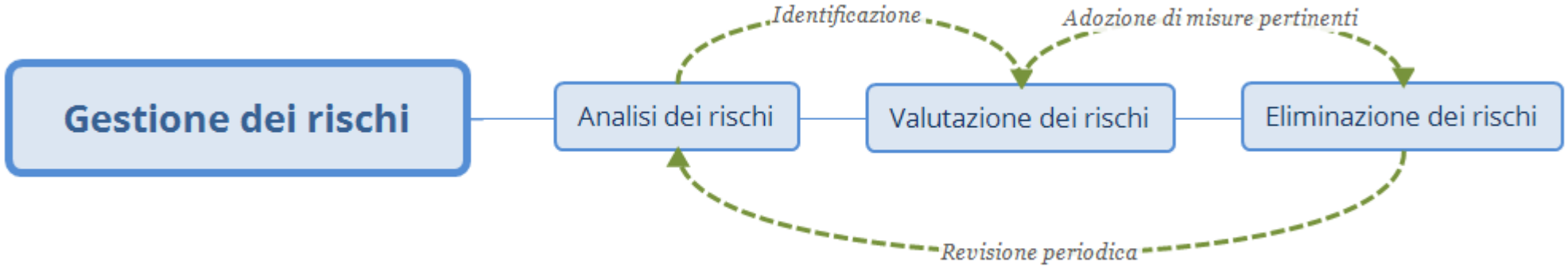
Riferimenti a standard

- NIST Guide to Industrial Control Systems (ICS) in particolare la gestione di sistemi di controllo industriali (ICS), NIST Special Publication 800-82, revisione 2, maggio 2015.
- ISO 2700x
- COBIT (Control Objectives for Information and related Technology)
- ENISA Good Practice Guide on National Cyber Security Strategies
- BSI 100-2, Bundesamt für Sicherheit in der Informationstechnik (Germania)

Gestione dei rischi

- La sicurezza informatica assoluta non esiste, è tutta una gestione di rischi, la direzione dell'organismo o dell'impresa deve pertanto stabilire quanti rischi è disposta ad assumere.

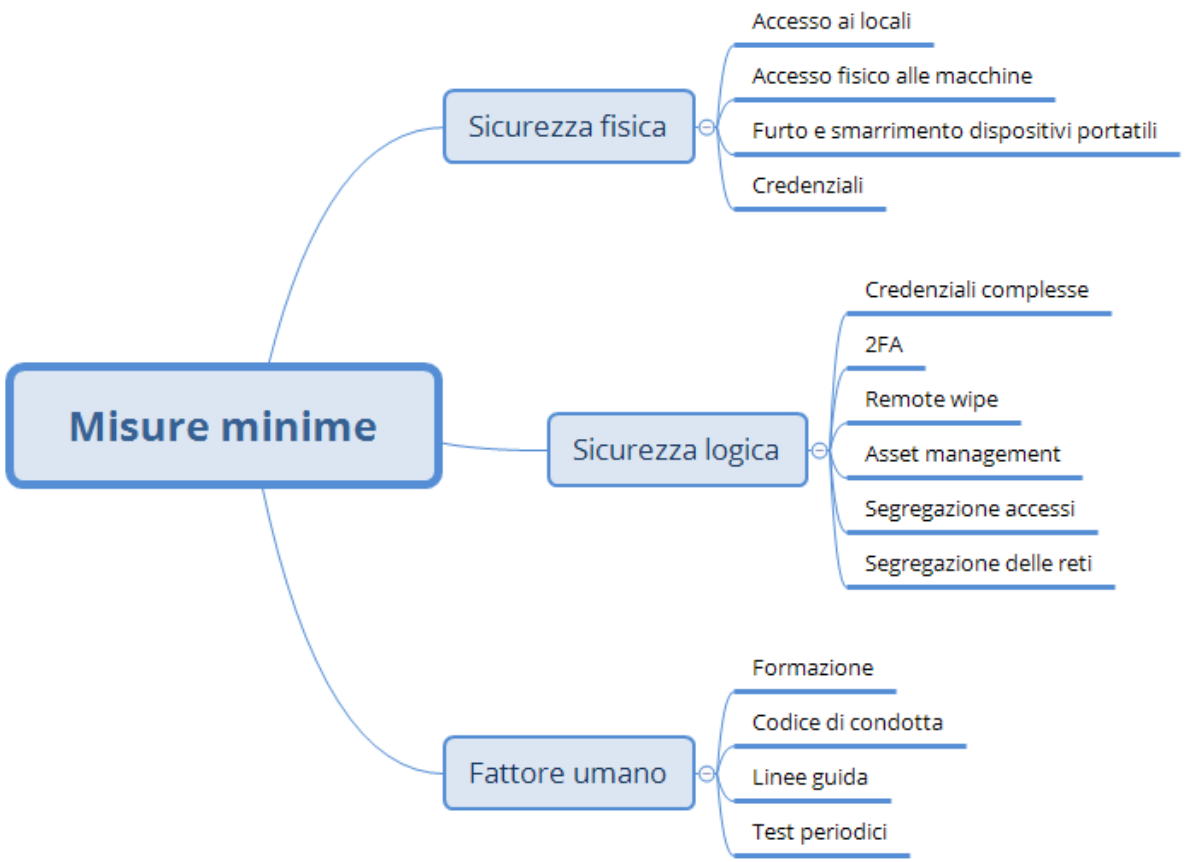
Si procede con tre fasi:



Defense-in-depth

- impiego coordinato di più misure di sicurezza atte a proteggere gli strumenti operativi TIC
- si basa su un principio militare, secondo cui per il nemico è più difficile superare un sistema difensivo complesso e stratificato rispetto a un'unica barriera
- analizza metodi e procedure dei potenziali attaccanti per preparare opportuni dispositivi di difesa
- Le risorse dell'organismo o dell'impresa vanno utilizzate in modo da garantire una protezione efficace da rischi noti e tenere ampiamente sotto controllo quelli potenziali

Cosa bisogna considerare?

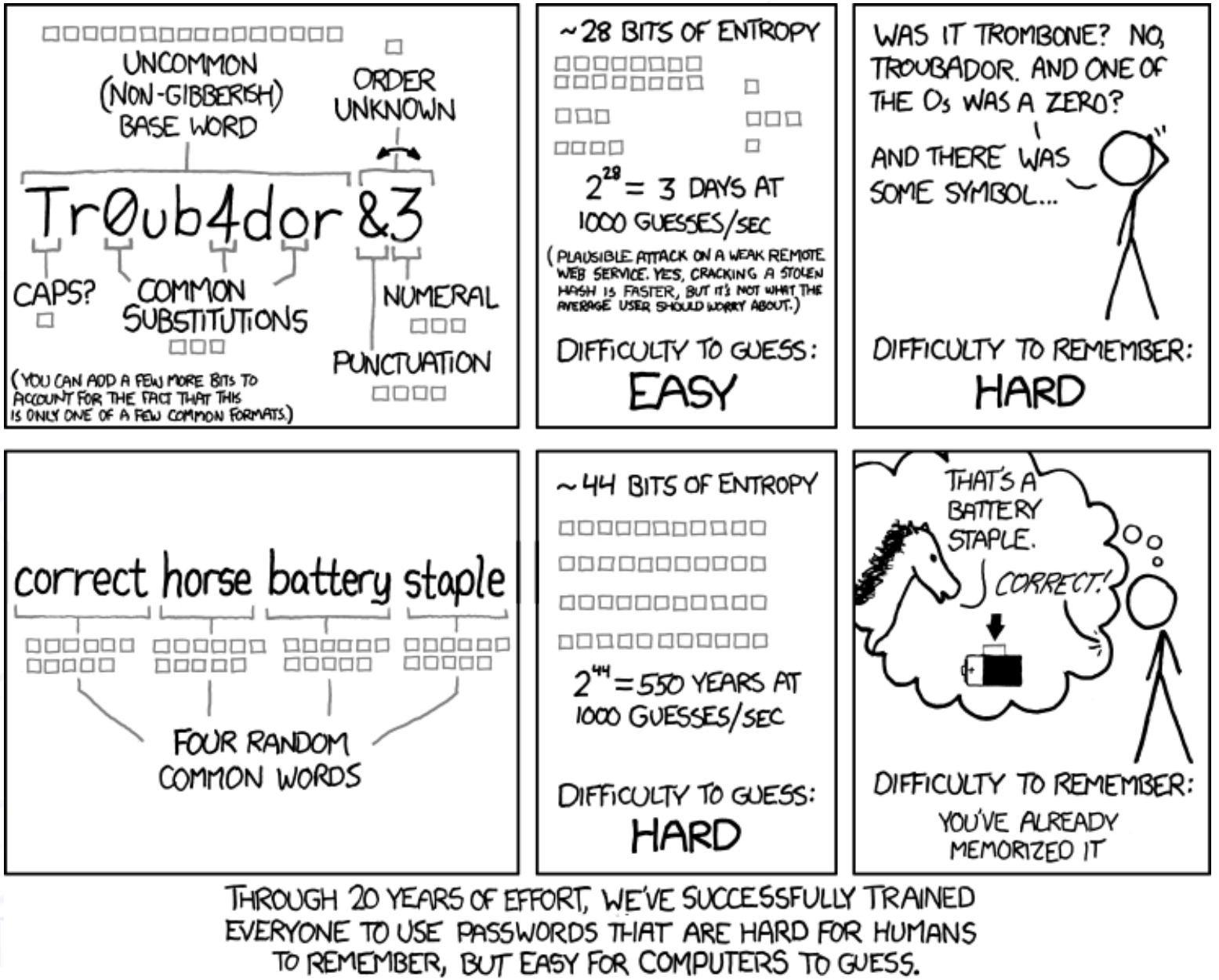


Password

Spesso viene richiesto l'uso di password complesse con risultati nefasti.

Alla fine gli utenti non le ricordano, le scrivono, magari su post-it, magari sotto la tastiera…

Questo va a braccetto con la formazione che è uno strumento necessario per la sicurezza.



Soluzioni

- 2FA;
- password manager;
- biometria; (possibili problemi normativi legati a trattamento dati biometrici, deve essere commisurato)
- smart card; (debole al furto)
- gestione password centralizzata; (no riuso, no modifica parziale, obbligo al cambio periodico)
- SSO (laddove strettamente necessario).

Problemi legati al fattore umano

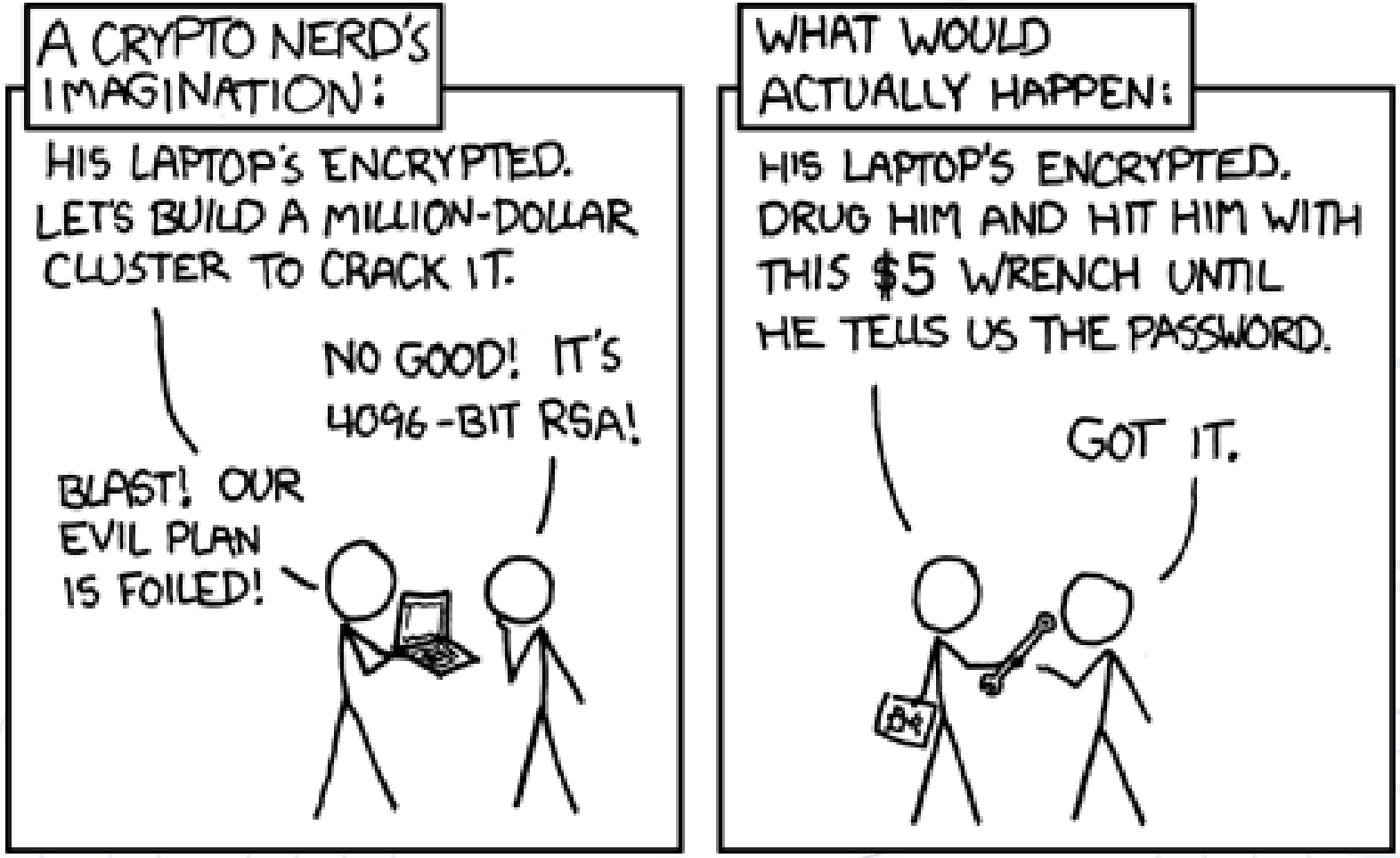
- inserimento dispositivi USB di dubbia provenienza;
- social engeneering;
- phishing;
- comunicazione di credenziali;
- conservazione credenziali;
- condivisione delle credenziali;
- errori;

Possibili soluzioni

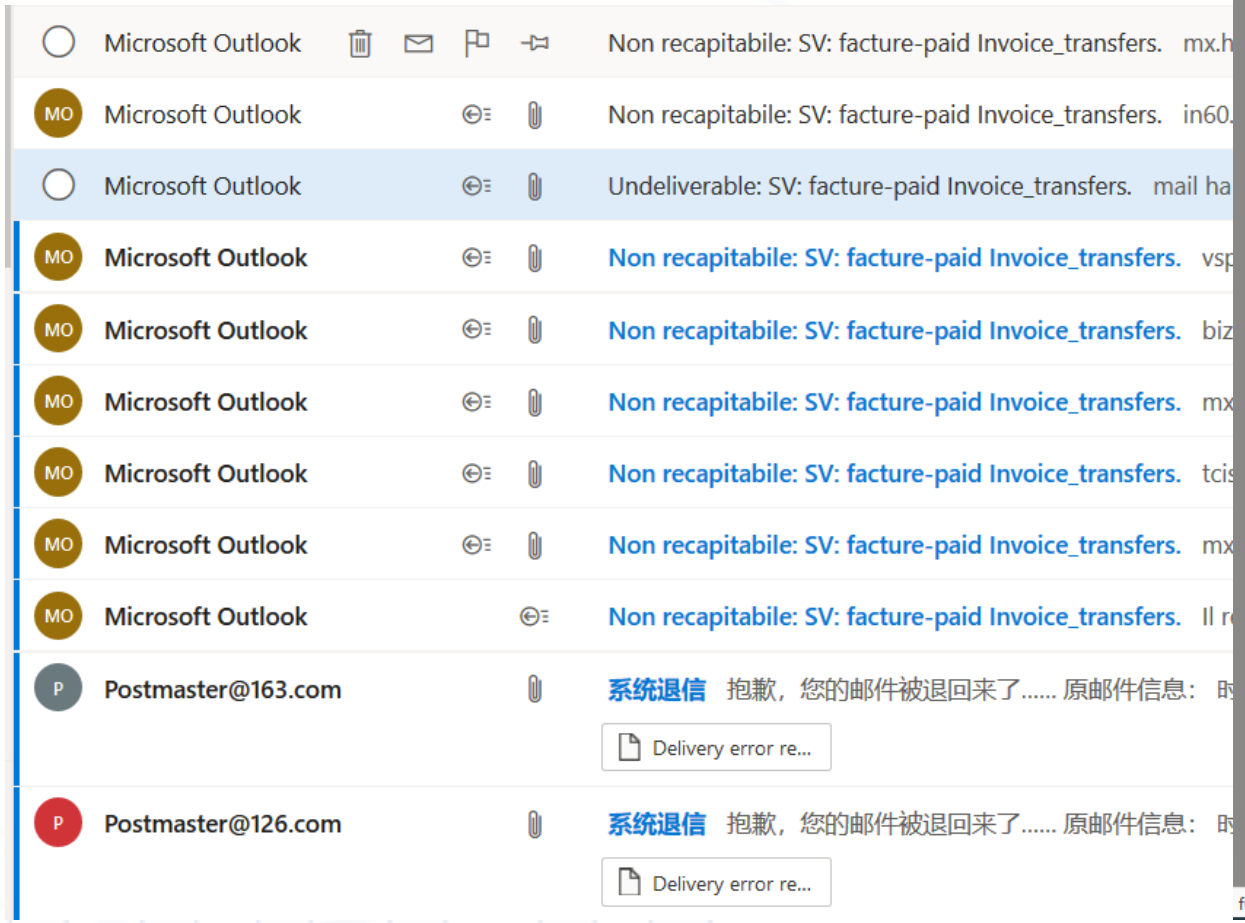
- remote wipe; (protegge da data-leak dovuti a smarrimento di dispositivi o furto degli stessi)
- device management; (controllo attivo sui dispositivi in uso agli utenti)
- sicurezza attiva; (antivirus, antispam, IDS, ecc.)

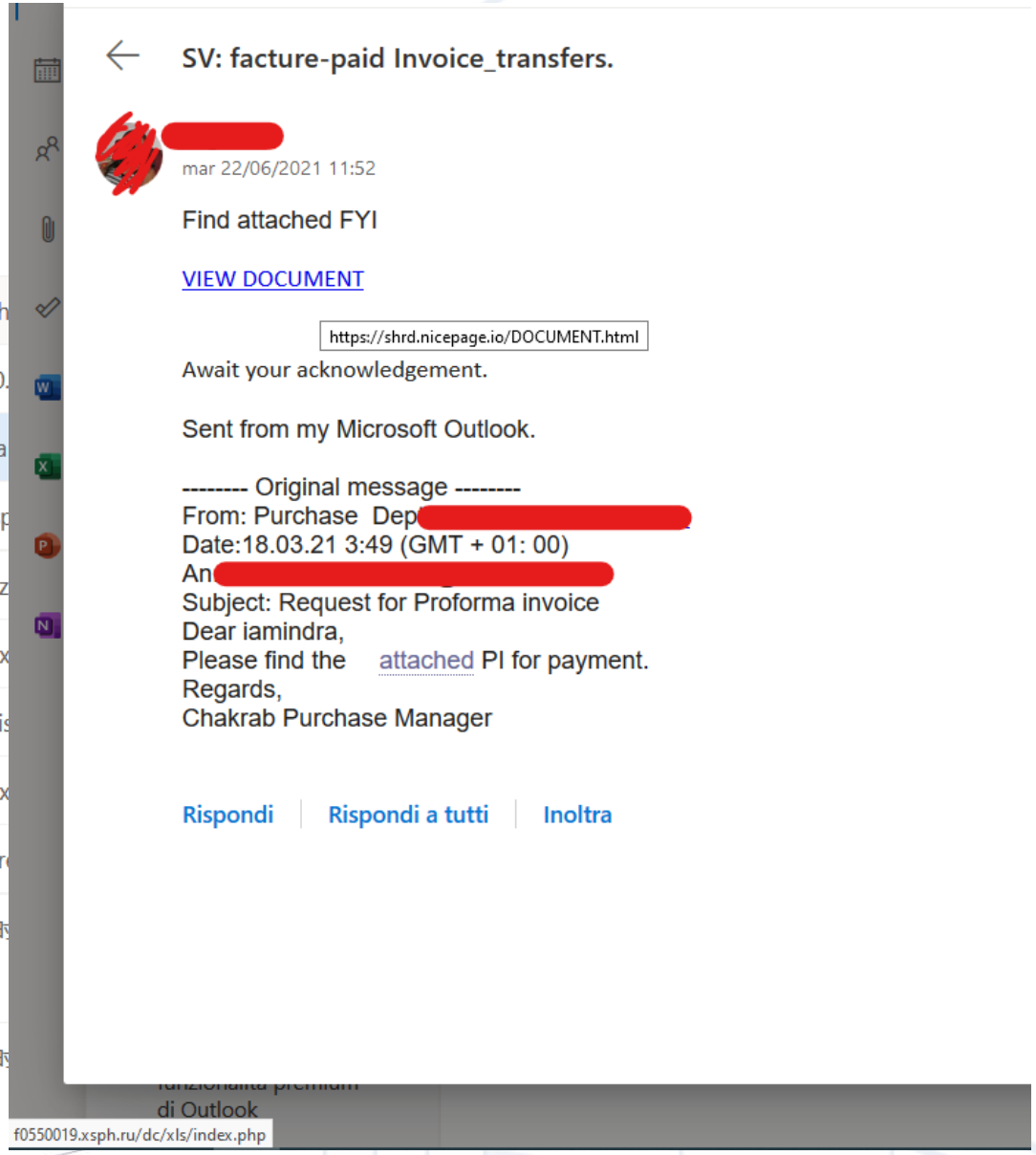
- **FORMAZIONE**

Fattore umano



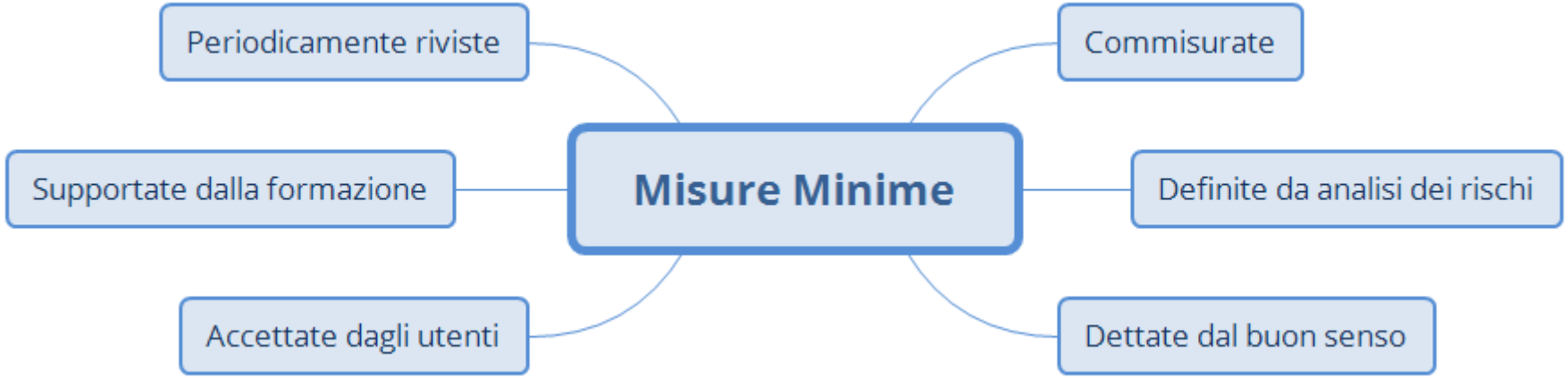
Fattore umano





In sintesi, quali sono le misure minime?

DIPENDE



Domande?

Comunicate in chat la volontà di intervenire e gestiremo le domande.

Offerta per il webinar

Mezz’ora di consulenza gratuita ai partecipanti, su appuntamento.

https://www.informatich.ch/prenota-un-appuntamento/

Grazie

InformatiCH Sagl

info@ellepidi.ch
www.informatich.ch
https://ellepidi.ch

+41 91 601 40 60
www.linkedin.com/company/informatich-sagl/