Aspetti umani, organizzativi e legali

Massimo Carnevali

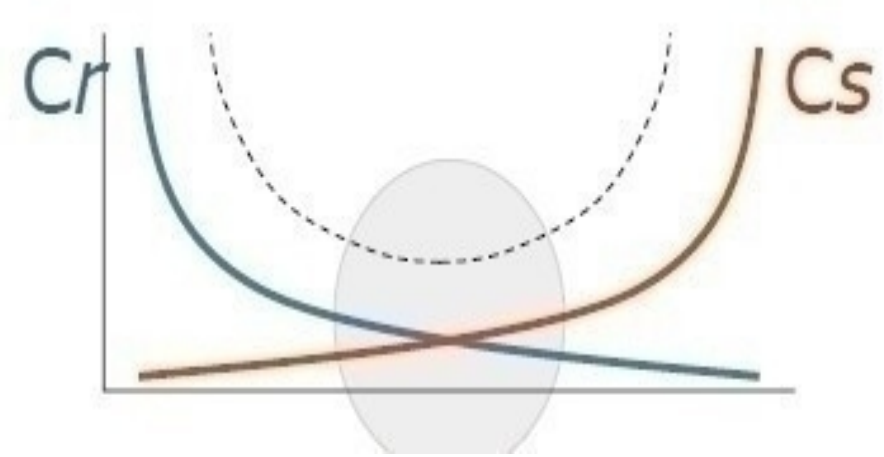
Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

Aspetti umani, organizzativi e legali

- Analisi dei rischi e bilancio costi-benefici-semplicità
- Il fattore umano
- BYOD e Shadow-IT
- Social Enginering
- Spam, Phishing e dintorni
- La gestione delle password
- Normativa vigente (GDPR)
- Certificazioni
- Cenni di gestione dei processi IT in ottica di sicurezza

.....

Costi vs analisi dei rischi



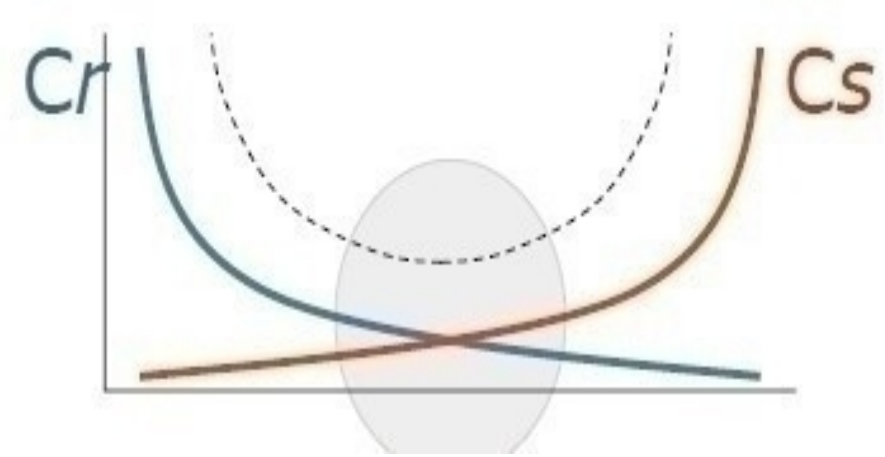
Nella definizione di un budget si esercita il tentativo di conciliare elementi contrastanti: il costo di un prodotto vs il beneficio previsto.

Nel caso di investimenti in sicurezza, come tutte le misure preventive, è spesso difficile quantificare il ritorno previsto; invece è più evidente come quantificare i costi. Si può cioè più facilmente ipotizzare un costo a cui si dovrebbe far fronte se non si adottano misure adeguate.

Disegnando qualitativamente le curve dei costi legati al rischio (Cr) e di quelli legati agli investimenti per la sicurezza (Cs), risulta evidente che il miglior compromesso è quello nell'intorno del minimo dei costi totali (linea tratteggiata=somma dei costi).

Analisi dei rischi

Modello Gordon-Loeb

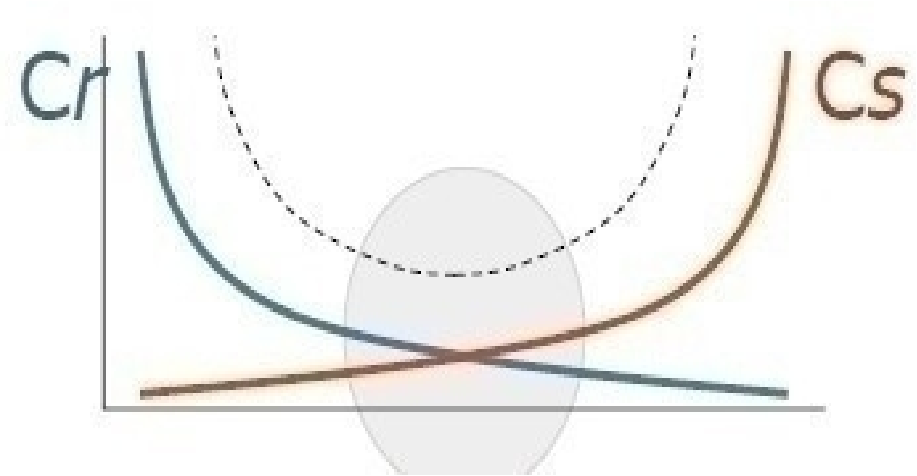


https://en.wikipedia.org/wiki/Gordon%E2%80%93Loeb_model

Quindi quando dobbiamo spendere?
Quanto vale il punto minimo della curva?
Secondo il modello Gordon-Loeb il valore giusto è intorno al 37% del valore dei danni in caso di perdita dei dati
“More specifically, the model shows that it is generally uneconomical to invest in information security activities (including cybersecurity or computer security related activities) more than 37 percent of the expected loss that would occur from a security breach.”

Analisi dei rischi

Rischio residuo



Come si vede dal grafico (e come dice il buonsenso) rimane sempre una quota di rischio residuo.

Tendenza recente: trasferimento del rischio residuo → assicurazione.

In Italia è ancora un mercato potenziale, è già molto attivo negli USA.

Non solo trasferimento economico ma anche supporto nei momenti critici.

Ovviamente bisogna leggere le clausole in piccolo ...

Analisi dei rischi

Sicurezza
=
Compromesso

Quindi la sicurezza non è un valore assoluto ma è un compromesso: “la spesa è commisurata al valore di ciò che sto assicurando?”

Ancora più complicato: “sto spendendo per essere al sicuro oppure per sentirmi sicuro?”

Facciamo continuamente scelte di questo tipo e l’evoluzione ci dice che dovrebbero sopravvivere quelli che le fanno giuste (ma non siamo tarati per le scelte del mondo presente).

Analisi dei rischi

La percezione della sicurezza

Security is both a feeling and a reality, and they're not the same.

- Alternative A: A sure gain of $500.
- Alternative B: A 50% chance of gaining $1,000.

- Alternative C: A sure loss of $500.
- Alternative D: A 50% chance of losing $1,000.

84% A vs 16% B
70% D vs 30% C

The Psychology of Security - Bruce Schneier

https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html

Rischio uguale in tutti e quattro i casi (guadagno o perdita statisticamente uguale).

https://www.ted.com/talks/bruce_schneier

Analisi dei rischi

Percezione vs realtà:

- Spettacolare vs comune
- Ignoto vs famigliare
- Identificato vs anonimo
- Controllo della situazione
- Media

Che cosa influenza il rapporto percezione/realtà?
1)Rischi spettacolari vs comuni (aereo vs auto)
2)Sconosciuto vs famigliare (violenza alle donne)
3)Identificato vs anonimo (ISIS vs ubriaco)
4)Controllo della situazione (terrorista vs auto o sigaretta)
5)Influenza dei media (Aviaria, meningite)
Sono tutti temi che si applicano anche alla cyber security:
1) mega attacchi vs perdita di dati
2) “i cattivi sono fuori” vs dipendente infedele
3) CIA/Russi/anonymous vs mille altri attaccanti
4) cloud vs server in casa
5)

Analisi dei rischi

Economia comportamentale

Teoria del prospetto

Decision #1:
A) 100% chance of receiving $3,000
B) 80% chance of receiving $4,000, 20% chance of receiving nothing

A expected outcome is $3,000 while B is $3,200 but 80% of subjects choose option A

Decision #2:
C) 100% chance of losing $3,000
D) 80% chance of losing $4,000, but a 20% chance of losing nothing

C expected outcome is losing $3,000 while D is losing $3,200. 92% of people choose D

https://en.wikipedia.org/wiki/Behavioral_economics

Economia comportamentale vs economia tradizionale: l'uomo reale non sempre sceglie la soluzione matematicamente migliore.

Teoria del prospetto: come scegliamo.

https://en.wikipedia.org/wiki/Prospect_theory

Non quella razionalmente più conveniente ma quella che ci fa soffrire meno.

L'attaccante opera nel dominio dei guadagni (A-B) mentre il difensore opera nel dominio delle perdite (C-D), questa asimmetria falsa le scelte strategiche.

Bisogna tenerne conto.

Economia comportamentale

Come decidiamo?

- Punto di riferimento
- Cerchiamo di evitare le perdite
- Non siamo lineari
- Poco sensibili ai grandi valori

- Cerchiamo un punto di riferimento e ragioniamo in base a quello (può essere diverso per attaccante e difensore, può muoversi a velocità diversa nei due casi)
- Cerchiamo di evitare le perdite (a parità di valore una perdita ci fa soffrire 2,25 volte più di quanto lo stesso guadagno ci faccia piacere)
- Non siamo lineari, sottovalutiamo le grandi probabilità e sopravvalutiamo quelle piccole (e preferiamo le certezze)
- Più lontano il guadagno o la perdita è dal punto di riferimento meno siamo precisi nei ragionamenti

Tutti fattori che influenzano le strategie di difesa: esempio 2 factor autentication, utenti amministratori dei PC, sarebbero comodi ma non si usano.

Articolo sul tema:
https://medium.com/@kshortridge/behavioral-models-of-infosec-prospect-theory-c6bb49902768

Analisi dei rischi

E poi guardiamo troppi (tele)film! (e ragioniamo poco)

I terroristi non guardano i film!
https://www.schneier.com/essays/archives/2005/09/terrorists_dont_do_m.html

Esempio di ragionamento fallace:

Se cerchi di salire in aereo con una pistola vieni fermato e identificato, magari finisci in blacklist o vieni arrestato, sicuro la seconda volta hai problemi.

Se hai una bottiglietta da 110cc te la tolgono. Punto. Puoi provarci tutti i giorni e non ne rimane traccia. Quindi puoi tentare all'infinito con una boccetta di esplosivo e prima o poi ci riuscirai.

Quindi ha senso togliere le bottigliette e basta?

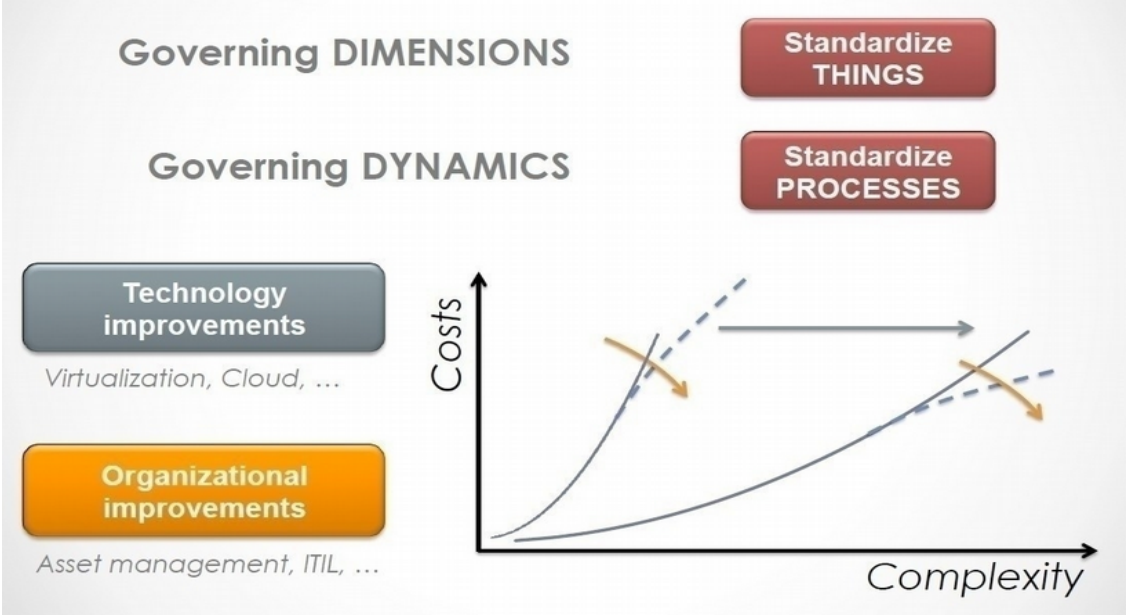
Di nuovo, non aumenta la sicurezza ma solo il senso di sicurezza.

Evoluzione e analisi della complessità

La complessità è nemica della sicurezza.
Per ridurre i rischi debbo ridurre anche la complessità.

Vi sono due dimensioni principali da percorrere per il raggiungimento del governo della complessità IT:
- la cardinalità dei fenomeni
- l'organizzazione del servizio.

Analisi dei rischi



Vi sono due dimensioni principali da percorrere per il raggiungimento del governo della complessità IT:

- la cardinalità dei fenomeni
- l'organizzazione del servizio.

Nella prima dimensione sfruttiamo la tecnologia per introdurre o accrescere la standardizzazione delle cose (ad esempio per ridurre il numero di modelli di computer impiegati: automatismi per l'installazione, virtualizzazione di server e client, ecc) e ottenere quindi una semplificazione nella gestione dell'installato.

Nella seconda sfruttiamo invece nuovi modelli o standard organizzativi, che consentono a gruppi di lavoro eterogenei e/o distribuiti di effettuare la gestione dell'installato

Analisi dei rischi

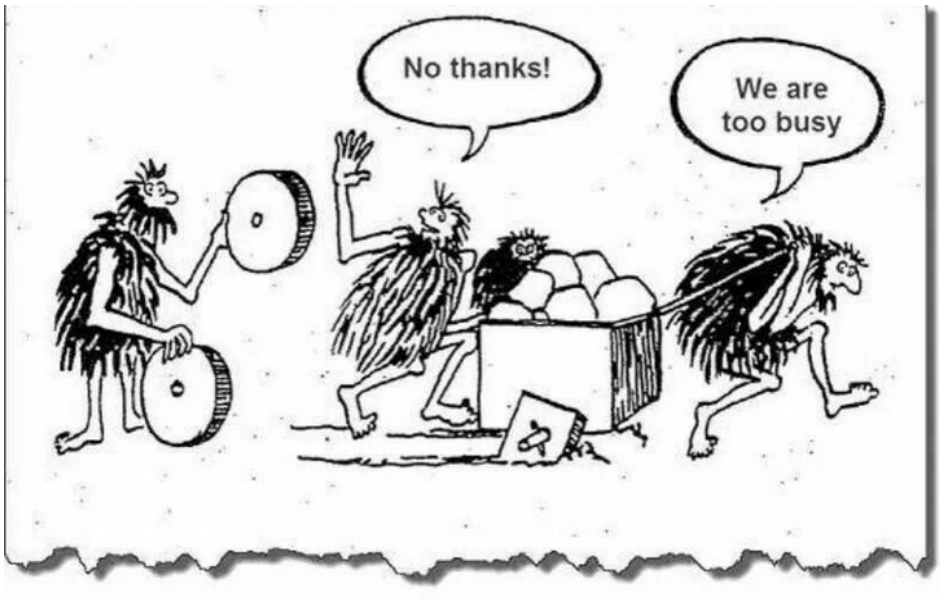
- Sicuro
- Economico
- Semplice

Analisi dei rischi

- Sicuro
- Economico
- Semplice

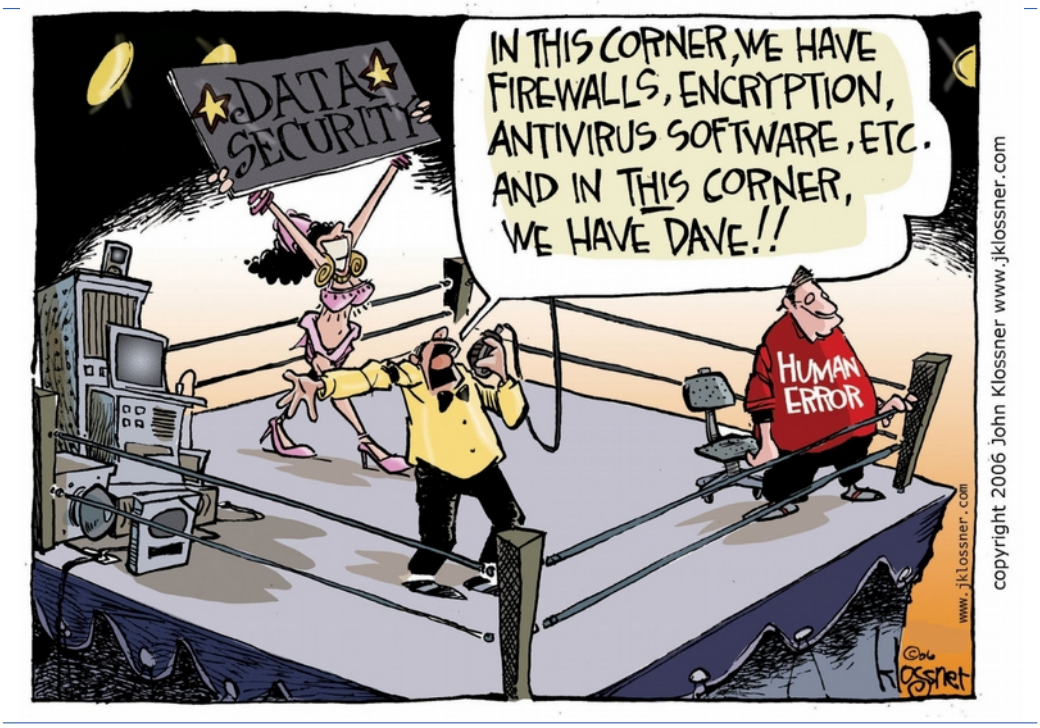
Scegline due!

Analisi dei rischi



Poi ovviamente c’è il problema di dover intervenire su ambienti “vivi”.

Il fattore umano



Ma siamo sicuri che l'utente "sbagli"?
O forse usiamo due modelli/linguaggi diversi?
Più che di "human error" spesso dovremmo parlare di "misunderstanding".
"Stop trying to fix the user"
https://www.schneier.com/blog/archives/2016/10/security_design.html

Il fattore umano

Tecnologia vs uomo/organizzazione

Anello più debole della catena = client/utente

“Se non conosci te stesso e non conosci il tuo nemico, sii certo che ogni battaglia sarà per te fonte di pericolo gravissimo.”
(Sun Tsu - L’arte della guerra)

Molti temi tecnologici hanno una loro controparte umana/organizzativa: sicurezza della navigazione, gestione dispositivi mobili, la posta elettronica, l'antivirus i salvataggi dei dati ecc.

“Se non conosci te stesso e non conosci il tuo nemico, sii certo che ogni battaglia sarà per te fonte di pericolo gravissimo.” (Sun Tsu - L’arte della guerra)

Attaccare i server e i DataCenter sta diventando sempre più complesso; è più facile provare a passare dal client e dall'utente finale, normalmente molto più fragili e attaccabili.

Problemi non tecnologici

- Awareness
- Fallibilità degli esseri umani
- Tendenza alla fiducia
- Interfacce/architetture complesse
- Prestazioni vs sicurezza
- Shadow IT
- BYOD

Problemi base (non tecnologici)

- Scarsa comprensione del problema (awareness)
- Fallibilità degli esseri umani (soprattutto in condizioni di sovraccarico, frustrazione, …)
- Gli esseri umani hanno una naturale tendenza alla fiducia
- Interfacce/architetture complesse che facilitano gli errori e lo stress nell'utente
- Calo di prestazioni dovuto all'applicazione delle misure di sicurezza (es. antivirus)
- Shadow IT (chi usa Dropbox in azienda? Il mio PC/ smartphone/tablet personale è meglio di quello aziendale! A volte il personale IT è fra i più indisciplinati!)
- da cui segue --→ BYOD

Shadow IT

https://en.wikipedia.org/wiki/Shadow_IT

Le applicazioni “consumer” ormai sono diventati più funzionali e performanti di quelle aziendali.

Social (Facebook) e posta personale completano il quadro.

Sono applicazioni non facilmente identificabili ed eliminabili.

Spesso vanno incontro ad esigenze reali dell’utente ma introducono problemi di sicurezza.

Anche una chiavetta USB è “Shadow IT”.

Anche gli acquisti “extra IT” lo sono.

AWS può diventare un nemico dell’IT aziendale.

Inutile approcciarlo con le cattive, meglio collaborazione e dialogo (“se non puoi combatterli unisciti a loro” … ma entro certi limiti)

Shadow IT Managers

Anche detti “technology leaders”.
Lo “smanettone” di reparto.
Quello a cui chiedere consigli per il prossimo smartphone.
Coinvolgerli, farseli amici, pericoloso averli contro!

Bring your own device (BYOD)

- BYOT – BYOP – BYOPC - BYOC
- COPE vs POCE
- Aggredire il problema tecnologico ma anche quello organizzativo (e legale)

http://en.wikipedia.org/wiki/Bring_your_own_device

Varie declinazioni: “Bring your own technology (BYOT)”, “Bring your own phone (BYOP)”, “Bring your own PC” (BYOPC), “Bring your own cloud (BYOC)” ecc.

COPE (Company Owned, Personally Enabled) vs POCE (Personally Owned, Company Enabled)

Esistono strumenti per aggredire il problema tecnologico (ad esempio software di Mobile Device Management tipo AirWatch http://www.air-watch.com/), è molto più complesso aggredire quello organizzativo (e legale, ad esempio GPS)

BYOD e Shadow IT

Bring your own device

- Limiti e modalità di utilizzo
- Responsabilità
- Servizi, Applicazioni, Dati
- Analisi dei rischi dell'adozione
- Infrastruttura tecnologica
- Misure di sicurezza
- Politiche di licensing
- Sistemi di monitoraggio
- Procedure di gestione
- Strumenti di supporto

Definire i limiti e le modalità di utilizzo dei dispositivi mobili non aziendali (o aziendali, quando abilitati anche all'uso personale).

Definire le responsabilità aziendali e quelle personali nell'uso dei dispositivi misti (responsabilità diverse nei casi di POCE vs COPE).

Definire i servizi, le applicazioni e i dati che devono essere accessibili dai dispositivi.

Fare un'analisi dei rischi dell'adozione del BYOD.

Definire l'infrastruttura tecnologica, le misure di sicurezza, le politiche di licensing, i sistemi di monitoraggio, le procedure di gestione e gli strumenti di supporto

BYOD e Shadow IT

Quindi sei l'Amministratore Delegato e vorresti installarti Instagram sullo smartphone aziendale?

- Identità = so chi sei
- Contatti = so chi conosci
- Posizione = so dove sei
- Fotografie = so cosa ti piace (cosa mangi)
- Archivio = so tutta la tua storia
- Fotocamera = magari ti faccio anche una foto
- Microfono = ti ascolto durante un CDA
- Batteria = so quando sei irraggiungibile (o posso renderti tale)
- Vibrazione/notifiche = so quando ti chiamano

Sono te!

BYOD e Shadow IT

Esistono anche strumenti più sofisticati di controllo dei dispositivi.

App che consentono il controllo totale da remoto di un dispositivo. Serve un breve contatto fisico con il dispositivo sbloccato. Illegali in Italia senza il consenso del controllato (se dipendente deve essere avvertito, comunque da contrattare con i sindacati come i sistemi di video sorverglianza, applicabile ai figli minorenni).

- https://www.flexispy.com/
- https://www.theonespy.com/iphone-spy-software/
- http://spyera.com/iphone-spy-app/
- https://www.mspy.it/
- http://www.highstermobi.com/

Social engineering

- Sfruttare l'utente
- Attaccare i punti deboli
- Pressione psicologica
- Utenti esperti!
- Molteplici canali di attacco
- Studio e analisi
- Conoscenza porta a fiducia

http://en.wikipedia.org/wiki/Social_engineering_(security)

Sfruttare la partecipazione (inconsapevole) dell'utente per un attacco.
Si cerca di attaccare i punti deboli dell'utente (vedi dopo).
Meccanismi di pressione psicologica (Nigerian Scam http://en.wikipedia.org/wiki/419_scams)
A volte ci cascano anche utenti esperti.
Sfrutta molteplici canali di attacco (mail, telefono, comunicazioni cartacee, chiavette USB ecc.).
Per riuscire bene richiede una fase di studio e di analisi molto accurati (attenzione a quello che racconta di noi il nostro sito web, i social ecc.)
Dimostrare di conoscere bene l'azienda, le persone, le procedure porta istintivamente il target dell'attacco ad abbassare la guardia.

Social engineering

I punti deboli dell'utente

- Coerenza
- Curiosità
- Validazione sociale
- Liking
- Autorità/Autorevolezza
- Scarsità
- Altruismo

Elementi comportamentali attaccabili:

- Coerenza: stabilità dei propri comportamenti e delle proprie convinzioni
- Curiosità: "chissà cosa c'è in questa chiavetta che ho trovato al bar..."
- Validazione sociale: "lo fanno tutti..."
- Liking: si tende a dare fiducia a chi è simpatico, bello o gentile
- Autorità/Autorevolezza: esiste una sudditanza di base verso l'autorità vera o presunta
- Scarsità: si tende a sovrastimare il valore di una cosa potenzialmente scarsa
- Altruismo: siamo tendenzialmente portati ad aiutare una persona in difficoltà

Social engineering

I punti deboli dell'utente

- Reciprocità
- Senso di colpa
- Paura
- Ignoranza
- Avidità

Elementi comportamentali attaccabili:

- Reciprocità: se mi fai un regalo o mi risolvi un problema sono predisposto a ricambiare
- Senso di colpa: mi fai sentire in colpa per spingermi ad un comportamento
- Paura: reazioni istintive prevedibili in situazioni di panico
- Ignoranza: sfrutto la tua ignoranza per farti sbagliare
- Avidità: ti prospetto una situazione apparentemente interessante

Social engineering

La ricostruzione di un attacco reale (sembra un film ma è basato su una storia vera):

Targeted Cyber Attack Reality - Trend Micro
https://www.youtube.com/watch?v=0hs8rc2u5ak

Costruire un attacco mirato partendo da quanto ricavabile dai Social Network:

Amazing mind reader – Safe Internet Banking - Belgio
https://www.youtube.com/watch?v=F7pYHN9iC9I

https://www.youtube.com/watch?v=0hs8rc2u5ak

https://www.youtube.com/watch?v=F7pYHN9iC9I

Molti esempi e storie interessanti in “The Ultimate Guide to Social Engineering” From CSO Magazine

Social engineering

Un esempio personale:

Esempio di social engineering telefonico
https://www.youtube.com/watch?v=lc7scxvKQOo

Lettura istruttiva

L'arte dell'inganno - Kevin David Mitnick

https://it.wikipedia.org/wiki/L%27arte_dell%27inganno

Oppure Robert B. Cialdini: Le armi della persuasione.
https://www.youtube.com/watch?v=CdZrgnf12v0

A seguire: Kevin David Mitnick, L'arte dell'intrusione
https://it.wikipedia.org/wiki/L%27arte_dell%27intrusione

Social Engineering + domini DNS = colpo da 40M€

LEONI

COMPANY

16 Aug 2016 [Ad-hoc announcement] [Company]

Leoni targeted by criminals

Nuremberg: Leoni AG (ISIN DE 0005408884 / WKN 540888) realised on Friday 12 August 2016 that it had become the victim of fraudulent activity with the help of falsified documents and identities and the use of electronic communication channels. As a result, company funds were transferred to accounts abroad. The Management Board immediately launched an investigation into the events and is currently assessing claims for damages and insurance claims. It has also reported the matter to the police criminal investigators. The damage amounts to an outflow of liquidity totalling around EUR 40 million. The criminal activities have not affected the IT infrastructure or data security.

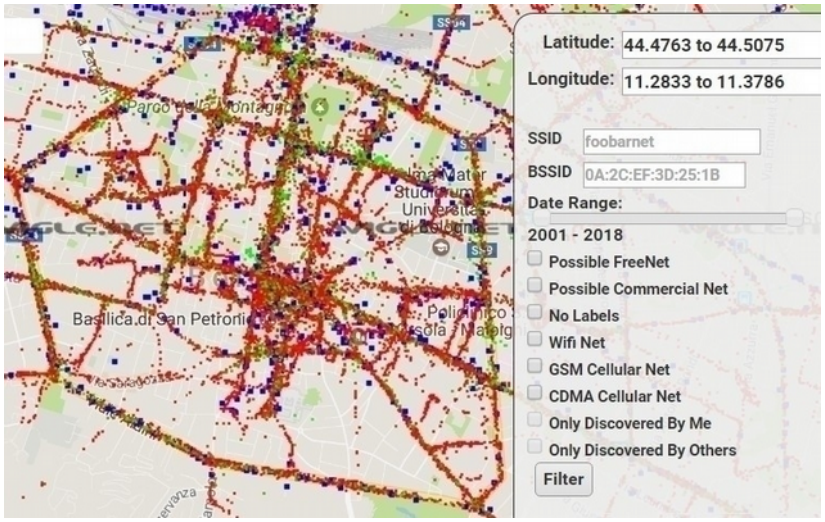
The extent to which the damage will affect the projected net income for the year cannot at present be assessed. The liquidity situation of the Leoni Group has not been adversely affected in any material way. The performance of Leoni's operations is in line with the forecast.

https://www.leoni.com/en/press/releases/details/leoni-targeted-by-criminals/

"The extent to which the damage will affect the projected net income for the year cannot at present be assessed. The liquidity situation of the Leoni Group has not been adversely affected in any material way."

Oltre al danno diretto anche i danni collaterali.

Il tuo telefono fa la spia (e racconta dove sei stato)



Il telefono ogni tanto esegue una “probe request” cercando le reti wifi che già conosce per collegarsi.
https://www.crc.id.au/tracking-people-via-wifi-even-when-not-connected/

Dal nome delle reti si ricostruisce la storia del telefono (Starbucks, McDonald ecc.) e si può risalire all’abitazione del proprietario con siti come WIGLE https://wigle.net/

Raccolta dati tramite Wardriving
https://en.wikipedia.org/wiki/Wardriving
(o tramite Google ….)

Anche indoor (meglio con il BT)

TODAY'S TOP STORIES

Virtual beacons challenge Wi-Fi for in-building, location-based supremacy

Bluetooth Low Energy (BLE) beacons from Mist Systems and Cisco could revolutionize the consumer experience in retail, healthcare, hospitality.

By Craig Mathias
Principal, Network World | MAR 27, 2017 3:00 AM PT

Possibilità di tracciare utente indoor tramite wifi (“new Wi-Fi positioning standard, 802.11az, is now under development, promising improved accuracy and perhaps even introducing the possibility of a Wi-Fi positioning ecosystem”) con precisione di un metro. Già in uso anonimizzato in aeroporti.

Es. supermercato ti manda offerte in base allo scaffale.

Ulteriori sviluppi usando Bluetooth che consuma meno, costa meno ed è più preciso. Virtual Beacon.

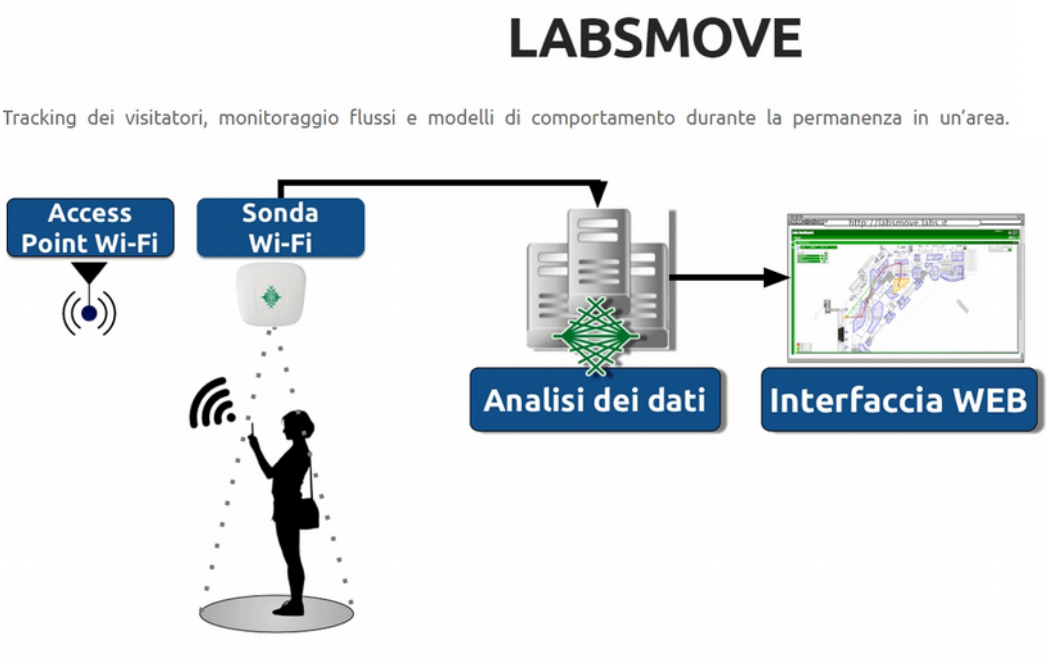
Un incrocio fra i due: https://www.mist.com/

http://www.networkworld.com/article/3183581/mobile-wireless/virtual-beacons-challenge-wi-fi-for-in-building-location-based-supremacy.html

Social engineering

Il supermercato che ti segue mentre fai la spesa (esiste già)

Social engineering



In aeroporto esiste già.
Www.labs.it
Ovviamente è anonimizzato ma è solo un tema giuridico, tecnicamente si potrebbe inseguire la singola persona.
Loro non lo fanno, i cattivi invece?

Social engineering

Anche mentre guardiamo una vetrina

Le tue fotografie fanno la spia

GPS information:	
GPSVersionID	2.2.0.0
GPSLatitudeRef	N
GPSLatitude	39 54 56 (39.915556)
GPSLongitudeRef	E
GPSLongitude	116 23 27 (116.390833)

Se attivo i servizi di geolocalizzazione sullo smartphone anche le fotografie registrano la posizione.

EXIF (visualizzabile ad esempio con Irfanview http://www.irfanview.com/ o con servizi online)

Data, ora, tipo fotocamera ma anche coordinate GPS.

I social DOVREBBERO filtrare questo dato in fase di caricamento.

Tool per estrarre dati dalle immagini e per analizzarle (se modificate con photoshop ecc.)

http://www.getghiro.org/

La tua carta d'imbarco fa la spia

Nel codice a barre bidimensionale ci può essere nome, cognome, indirizzo, telefono, carta di credito, utente del sito della compagnia aerea ecc.

Mai mettere la foto su internet, non buttarlo via integro.

https://krebsonsecurity.com/2015/10/whats-in-a-boarding-pass-barcode-a-lot/

Poi ci sono i geni assoluti….

https://twitter.com/needadebitcard

Spegnere il GPS non (sempre) aiuta

Anche con il GPS spento il telefono conosce il nostro fuso orario, misura pressione barometrica (e la confronta con i dati meteo in tempo reale, deduce l'altitudine), campo elettromagnetico, la velocità a cui ci stiamo muovendo (piedi, auto ecc.), le curve che facciamo (e le confronta con le mappe) ecc.

E' dimostrato che ci può trovare in poche decine di minuti.

http://ieeexplore.ieee.org/document/8038870/

https://www.schneier.com/blog/archives/2017/12/tracking_people_5.html

Social engineering

Spie insospettabili in casa

Roomba's Next Big Step Is Selling Maps of Your Home to the Highest Bidder

Rhett Jones
7/24/17 2:05pm • Filed to: INTERNET OF THINGS
213

https://gizmodo.com/roombas-next-big-step-is-selling-maps-of-your-home-to-t-1797187829

Poi smentito, poi ritrattato che chiederanno il consenso al proprietario, poi apparentemente chiuso il progetto. Ci crediamo?

Poi c'è anche la versione con microfono e telecamera attaccabile da remoto

https://gizmodo.com/hack-can-turn-robotic-vacuum-into-creepy-rolling-survei-1827726378

Wearable come nuova frontiera

European Commission orders mass recall of creepy, leaky child-tracking smartwatch

Hackers can talk to and locate the wearer, warns notice

I fitness tracker come nuova frontiera: GPS, condizioni fisiche, microfono, altoparlante ecc.

Wearable attaccabili, “Io faccio indossare al bambino così so dove si trova”

Basso costo= bassa sicurezza

https://www.theregister.co.uk/2019/02/04/european_commission_security_risks_kids_smartwatch

Spie insospettabili in casa

La bambola Cayla ritirata in quanto bucabile tramite bluetooth
https://www.cnet.com/news/parents-told-to-destroy-connected-dolls-over-hacking-fears/

Le registrazioni dell'orsacchiotto Cloudpets diffuse su internet
http://money.cnn.com/2017/02/27/technology/cloudpets-data-leak-voices-photos/index.html

Social engineering

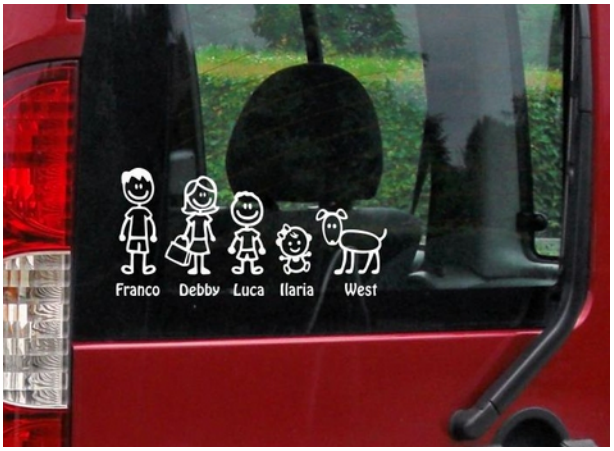
Suits allege Amazon's Alexa violates laws by recording children's voices without consent

June 12, 2019 at 11:38 am | *Updated June 13, 2019 at 3:59 am*

Assistenti vocali la nuova frontiera?
https://www.seattletimes.com/business/amazon/suit-alleges-amazons-alexa-violates-laws-by-recording-children-voices-without-consent/

I dipendenti di Amazon ascoltavano le registrazioni di Alexa "per migliorare l'algoritmo di riconoscimento vocale"

Social engineering



“ciao Ilaria, la tua mamma Debby è andata un attimo con il tuo papà Franco a prendere il tuo fratellino Luca a scuola, vieni con me che andiamo dal tuo cagnolino West che ti sta aspettando”

Sicuri di voler raccontare tutte queste cose?

Raccolta informazioni disponibili in rete
OSINT
Open Source Intelligence

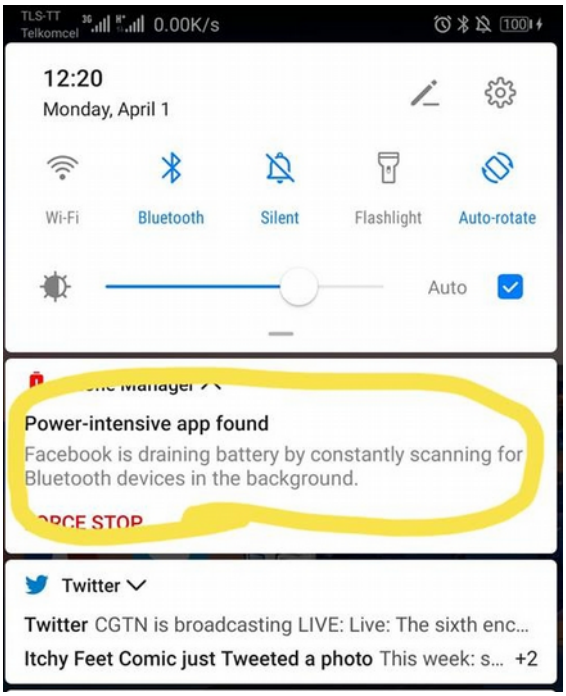
OSINT, raccogliere le informazioni in modo strutturato per fare attacchi Social Engineering (niente a che fare con FOSS!)
Distro apposita per fare ricerche
https://inteltechniques.com/buscador/index.html
Decine di tools online per farsi gli affari degli altri
http://osintframework.com/
Non nasce con internet ma ovviamente ha ricevuto un grande impulso con la diffusione delle banche dati più o meno aperte.

L’invadenza di PYMK

PYMK=People You May Know di Facebook
Algoritmo misterioso ma ci sono patent su “utenti nello stesso posto” (prostituta, i suoi clienti proposti alla sua identità pubblica), “utenti che si muovono assieme”, “imperfezioni simili in fotografie distinte, quindi stesso smartphone”, “abbiamo la stessa persona in rubrica”(pazienti di uno psichiatra) ecc.
https://gizmodo.com/
how-facebook-outs-sex-workers-1818861596
facebook-knows-how-to-track-you-using-the-dust-on-your-1821030620
facebook-figured-out-my-family-secrets-and-it-wont-tel-1797696163
tag/people-you-may-know

Social engineering

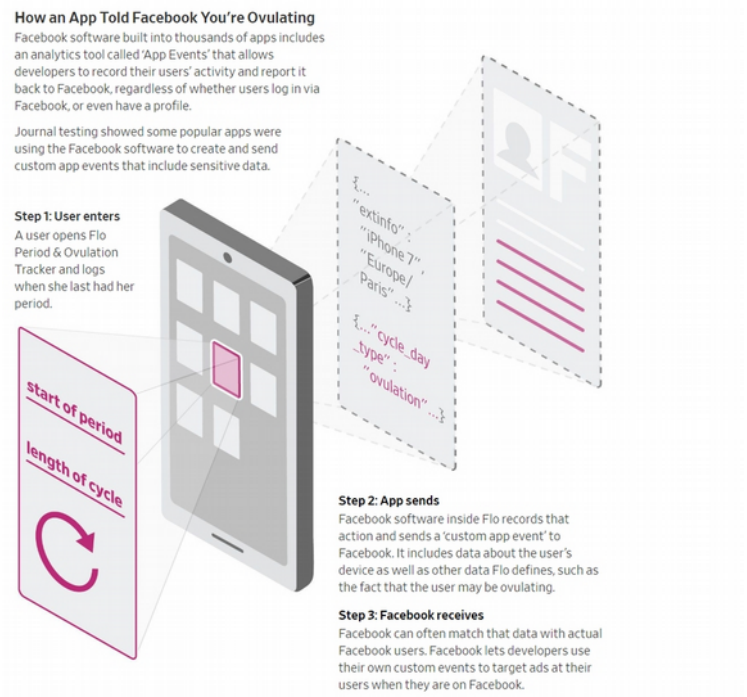
L’invadenza di Facebook



Quindi cerca dei bluetooth nelle vicinanze anche se non gliel’ho detto.

Social engineering

L'invadenza di Facebook



Smartphone Apps Sending "Intensely Personal Information" To Facebook - Whether Or Not You Have An Account

https://www.zerohedge.com/news/2019-02-22/smartphone-apps-sending-intensely-personal-information-facebook-whether-or-not-you

Spam

http://en.wikipedia.org/wiki/Email_spam

Lo spam, o “Unsolicited Commercial Bulk Email”, è un fenomeno largamente diffuso.

Da solo occupa buona parte della banda internet.

Consiste nel pubblicizzare prodotti e servizi a scopo commerciale o di phishing, o nell'indurre il destinatario della mail a visitare siti o pagine compromessi al fine di catturare dati o credenziali.

Produce danni sia come perdita di tempo che, a volte anche direttamente economici.

Non vi sono rimedi particolarmente efficaci o applicabili con elevato successo; tenendo alta l’attenzione all’evolversi del fenomeno si mettono in atto diverse pratiche, non ultima la “semplice” educazione degli utenti.

Spam, phishing e dintorni

Figure 10. This spam service offers support, just like many legitimate online offers.

Anche questo è ovviamente un business

http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf

Antispam

(strumenti base)

- Filtri sui contenuti
- Black&white-listing dei mittenti
- Graylisting

Vengono utilizzate varie metodologie per mitigare gli effetti dello spam (il punto finale dell'attacco rimane sempre l'utente finale):

Filtri sui contenuti (probabilistici e comunque sempre un passo indietro rispetto all'attaccante)

Black&white-listing dei mittenti (aggiornamento delle liste, rischio DOS per mittenti inconsapevoli)

Graylisting (rifiuto la prima mail con un “temporary error”)

Siti per verificare se sono finito nelle liste degli spammer (ad esempio http://mxtoolbox.com/blacklists.aspx)

Antispam

(strumenti avanzati)

- Sender Policy Framework
- DKIM
- DMARC (DKIM+SPF+Regole)

Sender Policy Framework (Controllo incrociato IP: se IP mittente non corrisponde IP in SPF record allora spam.)
https://en.wikipedia.org/wiki/Sender_Policy_Framework
Tool per validare:
http://www.kitterman.com/spf/validate.html
Problemi: gestione e propagazione

DKIM (DomainKeys Identified Mail) è un metodo tramite il quale il proprietario di un dominio “certifica” di prendersi la responsabilità di quella specifica email.

DMARC: DKIM+SPF+regole ulteriori
Va oltre SPF ma è ancora poco diffuso
Tool per validare o costruire record DMARC
https://dmarcian.com/dmarc-inspector/

Antispam

… oppure tenere occupato lo spammer

Chat/mail bot che tengono impegnato lo spammer in conversazioni fingendo di essere il target.
https://spa.mnesty.com/

Oppure se volete divertirvi…
https://www.ted.com/talks/james_veitch_this_is_what_happens_when_you_reply_to_spam_email?language=it#t-16339

Mail Marketing

Il confine fra SPAM e Mail Marketing può essere sottile.
“Mail non richiesta”, ma siamo sicuri che la richiesta sia sempre così esplicita? (Iscrizione a siti, scaricare documentazione, rispondere ad un invito ecc.)
Perché una email non finisca nello spam sono necessarie due condizioni:

1. Il server di invio deve **avere buona reputazione**, essere configurato correttamente e evitare di “infastidire” i domini di destinazione (nello spam ci mette il provider)
2. Il messaggio deve **essere non fastidioso** per i destinatari (nello spam ci mette l’utente)

Ricordarsi di mettere sempre le modalità di cancellazione dalla lista di distribuzione.

Phishing

http://en.wikipedia.org/wiki/Phishing

Neologismo, assonanza con “fishing” → “Andare a pesca di ingenui”. Via mail ma anche via IM.

Social Engineering di massa, spesso poco mirato, si lanciano milioni di esce sperando che qualcuno abbocchi.

Utilizzo di “shadow server”.

Metodologie di difesa simili a quelle contro lo SPAM.

Ancora più importante però la consapevolezza dell'utente.

A differenza dello SPAM la minaccia è nascosta e richiede un'azione da parte dell'utente.

Insegnare all'utente di cercare sempre il “lucchetto verde”.

Insegnare all’utente di diffidare di mail “strane” (“se non ho un contratto perché ricevo una fattura?”)

URL Shortner: http://www.trueurl.net/

Phishing

- Whaling
- Spear Phishing

Whaling: phishing mirato a CIO/CEO, molto sofisticato. C'è chi si è giocato il posto (FACC aerospatial Austria, frode da 40M€, licenziato CEO https://businessinsights.bitdefender.com/cyber-fraud-ceo-fired)

Spear Phishing: attacchi molto mirati a singole persone o gruppi, non necessariamente in alto nella catena gerarchica, ma potenzialmente canali di intrusione in azienda. Spesso l'anello debole della catena, alta percentuale di successo. Non esiste una risposta tecnologica → Awareness !

Verificate la vostra resistenza al phishing: https://www.opendns.com/phishing-quiz/

Le password:

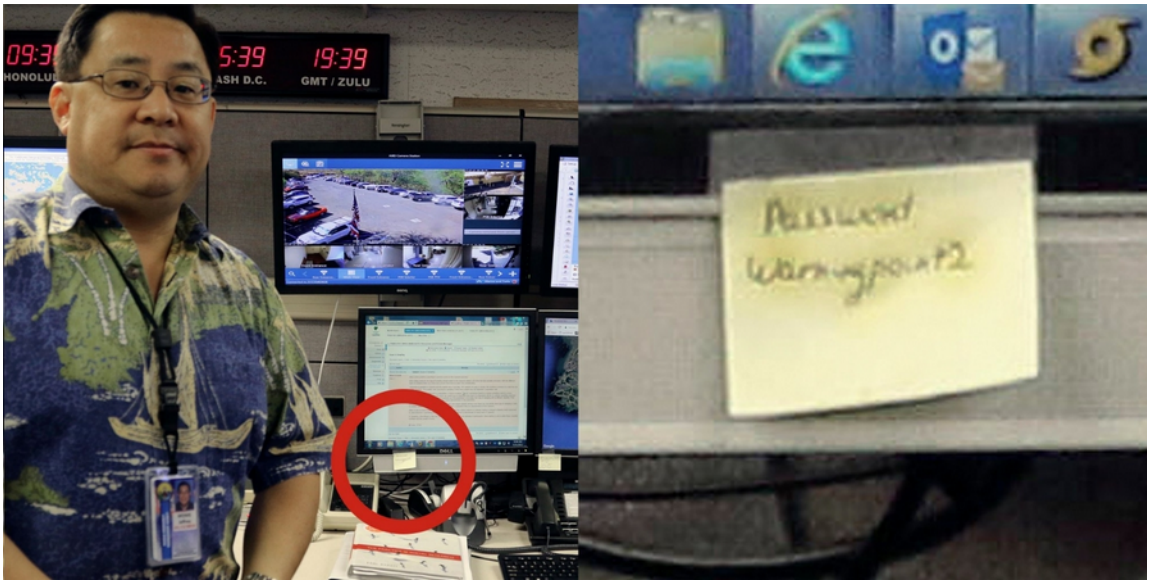
- Sono tante
- Non debbono essere ripetute
- Vanno conservate
- Andrebbero cambiate (NO! NO! NO!)
- Debbono essere difficili da indovinare

- Dobbiamo ricordare tante password (non usate la stessa in tutti i siti, vero?)
- Se vi beccano quella di un sito debole siete finiti (oppure se vi beccano quella del “recupera la tua password”)
- Non le scrivete su un foglietto giallo sotto la tastiera vero? Dove le conservate?
- Aveva senso una volta, ora non ha più senso, anzi induce confusione e abbassa la sicurezza. Vedi anche: https://www.schneier.com/blog/archives/2016/08/frequent_passwo.html

- No il nome del cane/gatto/figlio/moglie ovviamente

La gestione delle password

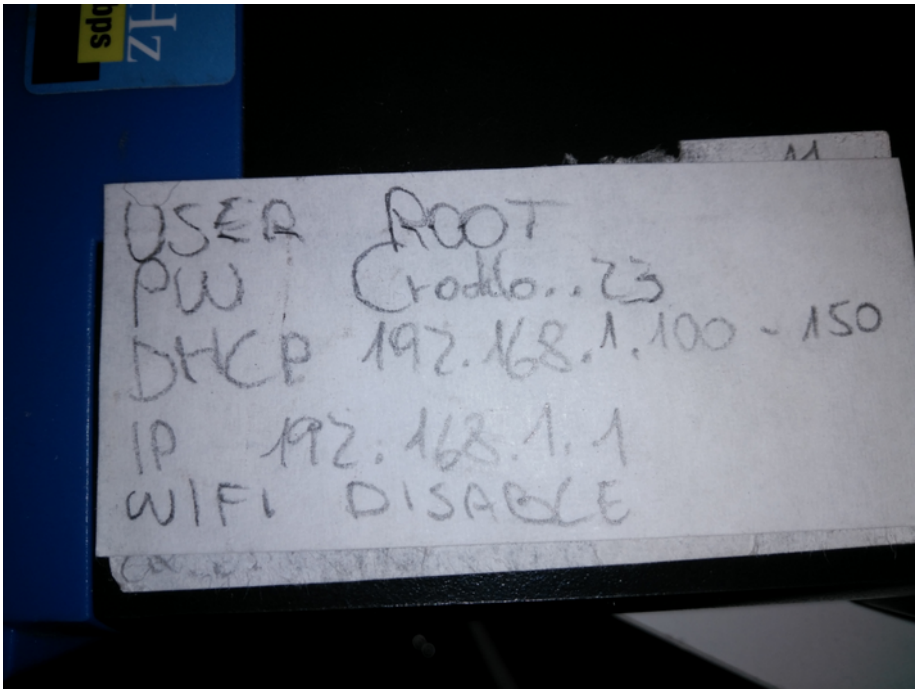
I foglietti gialli causa di allarmi nucleari



Gestisci gli allarmi nucleari degli USA nelle Hawaii, vieni intervistato e sui giornali di tutto il mondo si vede la tua password.

http://uk.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1?IR=T

La gestione delle password



.....

Una soluzione: Password manager

- In locale (Password Safe, KeePass ecc.)
- Nel cloud (1Password, LastPASS ecc.)

Ovviamente se vi perdete la master password siete finiti!

Esistono anche sistemi fisici (token usb) ma sono scomodi, possono essere persi e non sono supportati da tutti i software.

https://en.wikipedia.org/wiki/Comparison_of_password_managers

https://en.wikipedia.org/wiki/List_of_password_managers

Possono essere in locale oppure nel cloud, alcuni esempi:

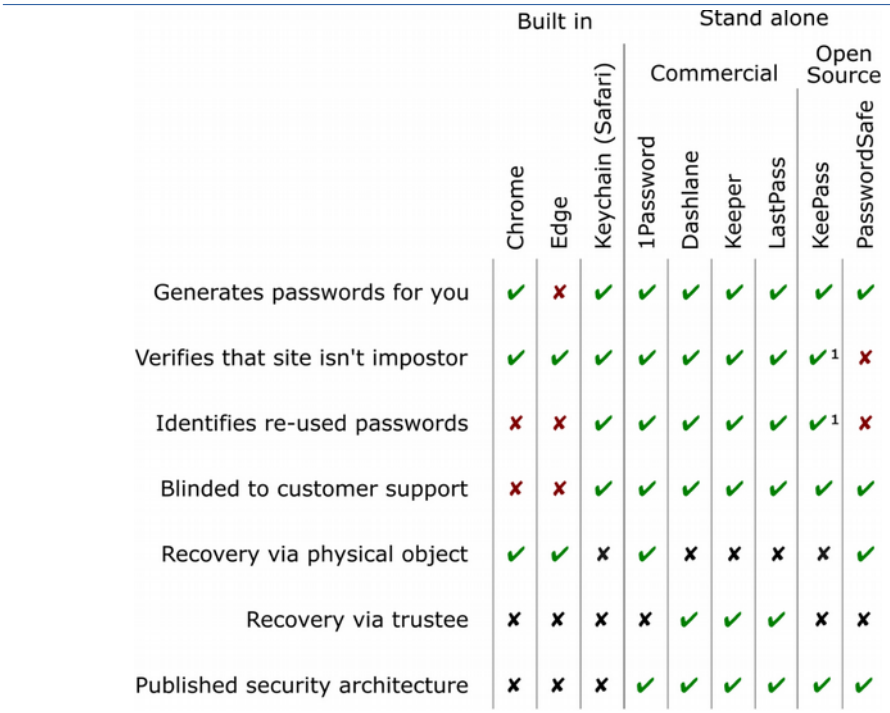
https://pwsafe.org/

http://keepass.info/

https://1password.com/

https://www.lastpass.com

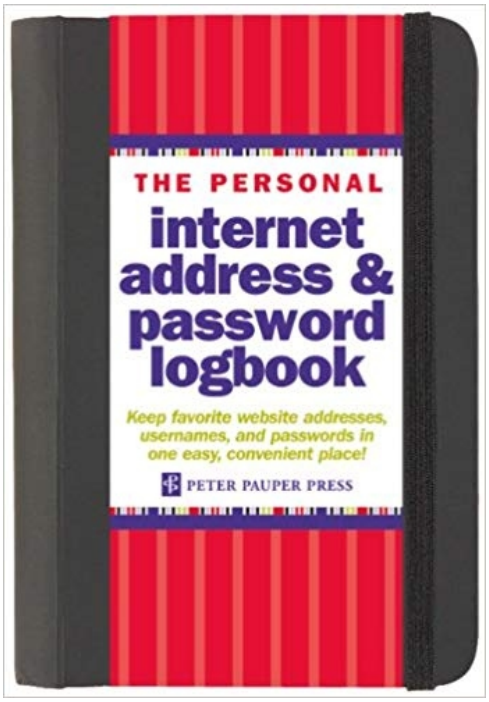
La gestione delle password



	Built in			Stand alone					
					Commercial			Open Source	
	Chrome	Edge	Keychain (Safari)	1Password	Dashlane	Keeper	LastPass	KeePass	PasswordSafe
Generates passwords for you	✔	✘	✔	✔	✔	✔	✔	✔	✔
Verifies that site isn't impostor	✔	✔	✔	✔	✔	✔	✔	✔[1]	✘
Identifies re-used passwords	✘	✘	✔	✔	✔	✔	✔	✔[1]	✘
Blinded to customer support	✘	✘	✔	✔	✔	✔	✔	✔	✔
Recovery via physical object	✔	✔	✘	✔	✘	✘	✘	✘	✔
Recovery via trustee	✘	✘	✘	✘	✔	✔	✔	✘	✘
Published security architecture	✘	✘	✘	✔	✔	✔	✔	✔	✔

Tabella riassuntiva dei principali password manager

Altra soluzione



Perchè no, se lo tenete in cassaforte…
(non è proprio comodo).
https://www.amazon.com/Personal-Internet-Address-Password-Book/dp/1441303251

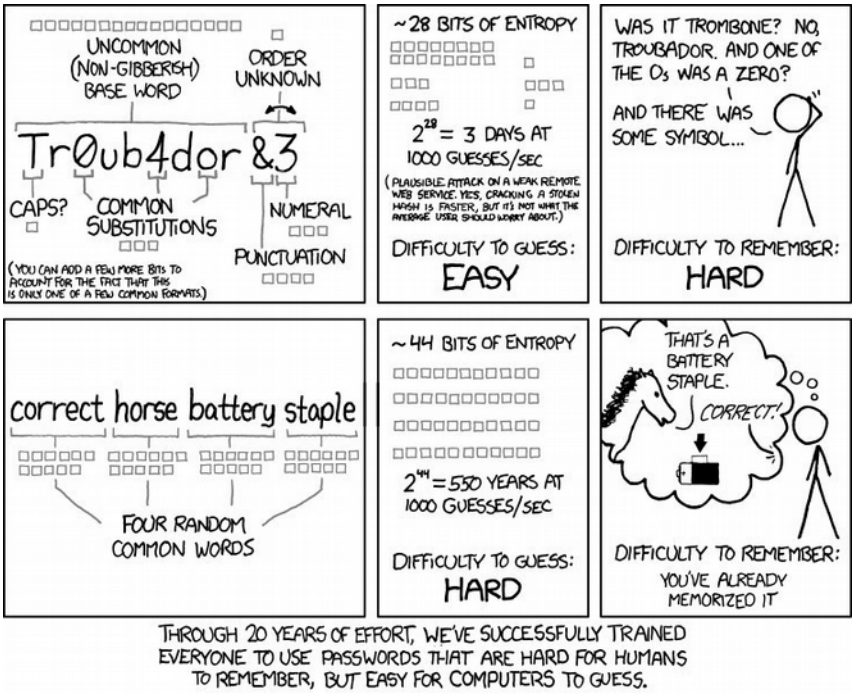
Ma se invece voglio avere una password sicura e memorizzabile? (master password ad esempio)

Almeno la master password però debbo ricordarmela e deve essere sicura.

Siamo certi che maiuscole/minuscole/caratterispeciali/numeri servano davvero?

La gestione delle password

Il falso mito delle password complesse



http://xkcd.com/936/

Vedi anche questo video:

https://www.youtube.com/watch?v=0SkdP36wiAU

Lo ha ammesso anche il suo creatore:

https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118

La gestione delle password

Esempio:

- Password di tre caratteri lettere o numeri = 42.875
- Se impongo almeno una lettera e un numero = 26.250
- Risparmio il 40% del tempo

Disposizioni con ripetizione

il numero delle possibili sequenze di k oggetti estratti dagli elementi di un insieme di n oggetti, ognuno dei quali può essere preso più volte = n elevato alla k

password di tre caratteri lettere o numeri
25+10 oggetti = n = 35
k=3
disposizioni = 42.875

almeno una lettera e un numero
42.875 - (password di sole lettere 25 alla 3) - (password di soli numeri 10 alla 3)
42.875 - 15.625 -1000 = 26.250 = 40% di tempo in meno attacco a forza bruta

La gestione delle password

Meglio se non contiene un segreto personale
Non deve dire la verità
Non deve avere senso
Non deve essere prevedibile
Le sostituzioni ovvie sono ovvie

E allora giochiamocela ai dadi!

- “amo Maria” ma mia moglie si chiama Giovanna
- Esiste una verità e tante bugie
- Per ogni frase sensata ne esistono di più senza senso
- “e poi ci troveremo come le ...”
- “s1cur0” non è più sicuro di “sicuro”

Diceware.
https://blog.agilebits.com/2011/06/21/toward-better-master-passwords/

*"'Source:'" Alexander Dreyer Two dices, all combination of eyes. Photographed by myself. {{self2|GFDL|cc-by-2.5}}

La gestione delle password

1) Lancio 5 dadi
2) Guardo la parola corrispondente nella tabella
3) Ripeto 4-5 volte
4) Costruisco una frase/immagine con le parole ottenute
5) (opzionale) sostituisco una delle parole con una mia personale (caratteri speciali ecc.)

4 parole + personale = 74 bit entropia
(500 Milioni anni a 1 milione tentativi/sec)

Diceware.
http://world.std.com/~reinhold/diceware.html
https://en.wikipedia.org/wiki/Diceware

Se interessa il calcolo dell'entropia e la matematica che c'è dietro:
https://blog.agilebits.com/2011/08/10/better-master-passwords-the-geek-edition/

La gestione delle password

One Time Password (password usa e getta)

OTP https://en.wikipedia.org/wiki/One-time_password
Con “token” fisico oppure con app su dispositivo.
Scomode, costose, deve essere un algoritmo veramente casuale
Problema allineamento dei clock (dispositivo-server, app-server, esempio token cambia ogni 60 secondi, deriva annua 15 secondi, ogni 4 anni debbo cambiare dispositivo)
Attacco DOS con ripetuti errori di chiave.
Attacco di Social Engineering per farsi sostituire la chiave.
2FA con SMS si attacca facendosi cambiare la SIM da un negozio compiacente/ingannato

Dispositivi HW o app

Ad esempio https://www.yubico.com
Bisogna averne almeno una di riserva.
Forte come il suo sistema di backup (“se hai perso la chiave ti faccio una domanda di recupero della password”)

Ad esempio Google Authenticator
Sostituisce chiavetta ed SMS, più affidabile se non perdo il telefono (che deve avere il pin ed essere cifrato ovviamente...)

Cenni (molto vaghi) sulla normativa vigente e sulle certificazioni

Cenni sulla normativa vigente

Tutti:
- Normativa per gli Amministratori di Sistema
- GDPR (General Data Protection Regulation (679/2016)
- Responsabilità amministrative degli enti D.Lgs. 231/2001
- Sicurezza sul lavoro (es. operatori VDT) D.Lgs. 81/2008
- Antiriciclaggio e reati finanziari D.Lgs. 231/2007
- Normativa sul diritto d'autore D.Lgs 633/1941 (?!)

Società quotate in borsa:
- Legge 262 (falsa informativa)
- Codice PREDA (danno reputazionale e impatto sul titolo)
- Regolamenti CONSOB

Settori specifici:
- Normative specifiche sui brevetti
- Normative sulla tracciabilità (GDO, alimentari, farmaceutici)
- Infrastrutture critiche
- Carte di credito e dati bancari

NON sono un giurista per cui il livello di dettaglio e il linguaggio sono da ingegneri!

Cenni sulla normativa vigente

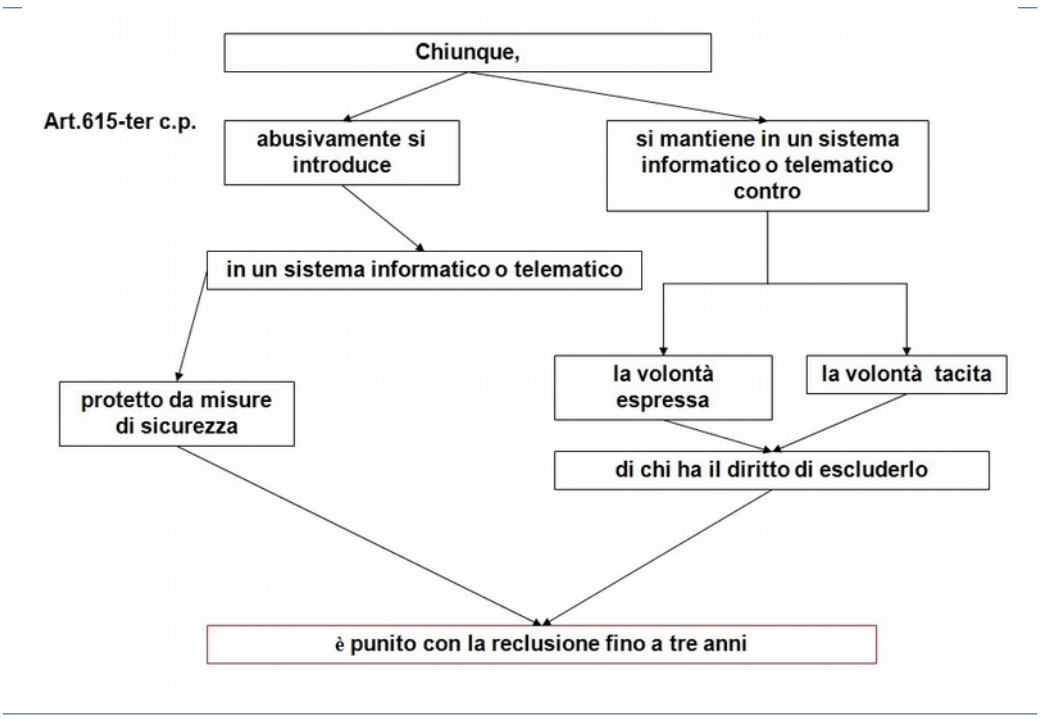
Normative per gli Amministratori di Sistema

- Identificazione e nomina degli amministratori di sistema
- Valutazione delle caratteristiche personali
- Diverso profilo giuridico
- Tenuta dei log delle operazioni svolte (inalterabile)
- Accesso nominale e non generico (root, admin ecc.)
- Problema in caso di servizi in outsourcing, insourcing, cloud ecc.

Testo:
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499

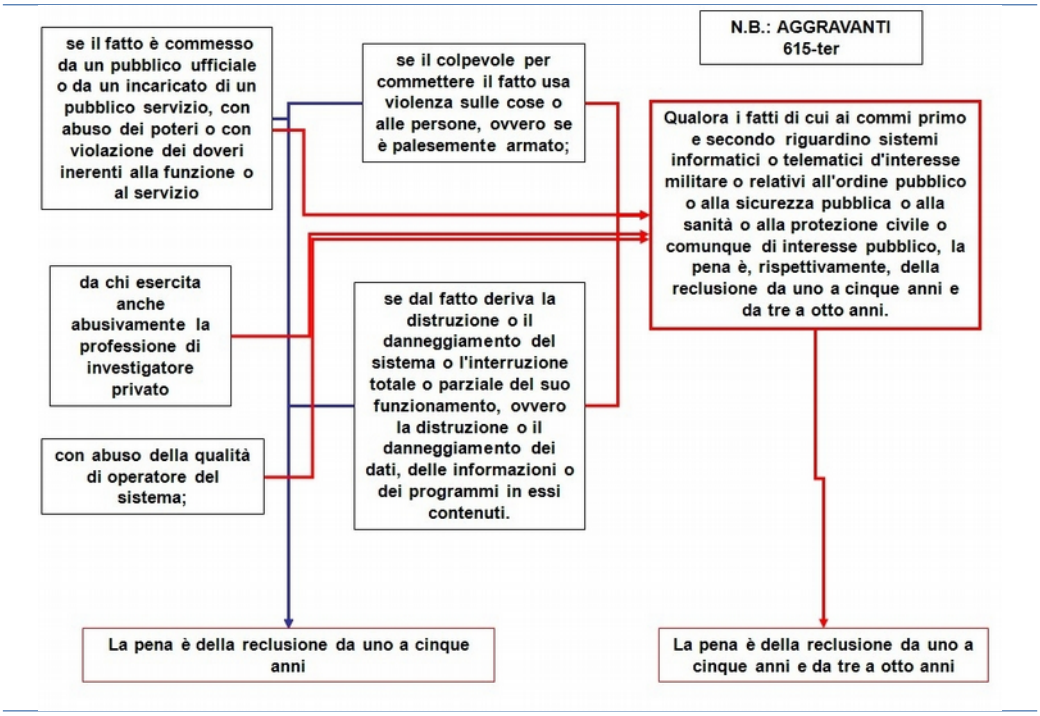
(non chiara la situazione ad oggi post GDPR)

Cenni sulla normativa vigente



Codice penale 615 ter (accesso abusivo) da 1 a 3 anni
Procedibile d'ufficio per la pubblica utilità (PA, banche, gestori telefonici, sanità ecc.) altrimenti richiede querela di parte entro 3 mesi da quando te ne sei accorto.
Prescrizione dai 6 ai 10 anni.
c.p 615 ter (accesso abusivo, ti ho bucato)
c.p 615 quater (ho le credenziali e le ho usate, la sola detenzione non autorizzata non basta, serve l'intento di usarle prima o poi)
c.p 615 quinques (creazione e diffusione malware a scopo di danno o profitto)
Se cedo le password a qualcuno che poi le usa è favoreggiamento.

Cenni sulla normativa vigente



Altro articolo correlato: codice penale 635 (danneggiamento informatico).
Cancellazione, deterioramento dati ecc. anche DDOS
Non è necessario che il danneggiamento ci sia, basta l'atto di cercare di farlo (es il mio antivirus ti blocca ma tu sei punibile lo stesso perché ci hai provato)

Vale il nuovo concetto di domicilio informatico (mia mail, mio facebook, mia cloud, tutto ciò che non è pubblico, condiviso solo fra amici).

https://www.youtube.com/watch?v=OzsD_PlG2aA

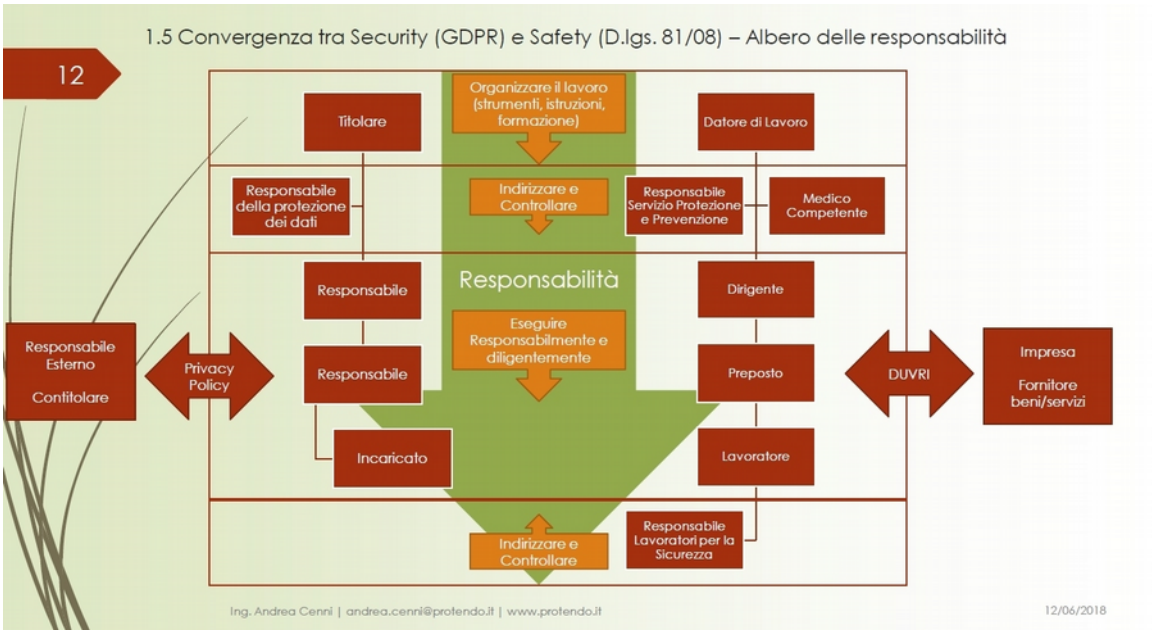
Cenni sulla normativa vigente

Regolamento 2016/679 EU Data Protection GDPR (General Data Protection Regulation)

- Normativa orientata alla sicurezza
- Valutazione del rischio, “misure adeguate”
- Regolamento europeo ma i singoli stati membri possono introdurre integrazioni nazionali
- Deroghe per aziende sotto i 250 dipendenti (semplificazione).
- Consenso e informativa
- Responsabile della protezione dei dati (Data protection officer)
- Registro dei trattamenti. Analisi dei rischi ed elenco trattamenti.
- Obbligo di segnalare violazioni dei dati personali (all'autorità di controllo e, in alcuni casi, agli interessati)

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Cenni sulla normativa vigente



. . . . .

Cenni sulla normativa vigente

Normativa sul diritto d'autore

D.Lgs. 633/1941 - Art. 96 Il ritratto di una persona non può essere esposto senza il consenso di questa + Art. 595 c.p. “diffamazione”

=

Reclusione da 6 mesi a 3 anni, multa non inferiore a 516€

https://it.wikipedia.org/wiki/Diritto_d'autore_italiano

Dà della Milf a collega su Facebook: è giusta causa di licenziamento: http://www.altalex.com/documents/news/2015/02/19/da-della-milf-a-collega-su-facebook-e-giusta-causa-di-licenziamento

Dare della Ninfomane alla propria “ex” su Facebook costa: http://www.comellini.it/H1.htm

Parere della cassazione sui reati a mezzo Facebook http://www.corrierecomunicazioni.it/ict-law/27313_diffamazione-massimei-la-cassazione-ha-dissipato-il-mistero-su-facebook.htm

Anzi è diffamazione aggravata vista la potenziale estensione della platea del messaggio: Cassazione penale Sezione V, 23/01/2017, n. 8482

Cenni sulla normativa vigente

Normativa sul diritto d'autore

- I software ma a volte anche le banche dati o i risultati prodotti dagli stessi software (si compera un supporto e una licenza d'uso non “il software”)
- Materiale audio, video, letterario protetto da diritto d'autore
- Verifica dei nomi a dominio, dei marchi, dei loghi
- Utilizzo materiale di terzi protetto da licenza

Due vie di uscita (da usare quando possibile)

Descrizione:
https://it.wikipedia.org/wiki/Diritto_d'autore_italiano

Non è una idea recente: Lo Statuto di Anna è stata la prima legge sul copyright in Gran Bretagna. È stato promulgato nel 1709 ed è entrato in vigore il 10 aprile 1710. E’ generalmente considerato il primo statuto completo sul copyright. Prende nome dalla regina Anna, durante il cui regno fu promulgato; oggi è considerato l’origine della legge sul copyright.
https://it.wikipedia.org/wiki/Statuto_di_Anna

Cenni sulla normativa vigente

Software Open Source

- “software distribuito con una licenza che ne consente la libera distribuzione in forma sorgente, e conferisce la possibilità all’utente di poter modificare il programma originario e di poter distribuire la versione modificata”
- Varie licenze, più famosa GPL
- “free speach, not free beer !”
- Le quattro libertà fondamentali del “Free software” sono:
  0) La libertà di eseguire il programma
  1) La libertà di studiare il programma, e adattarlo alle proprie necessità
  2) La libertà di distribuire copie
  3) La libertà di migliorare il programma e di rilasciare i propri miglioramenti al pubblico

https://en.wikipedia.org/wiki/Open-source_software

Cenni sulla normativa vigente

Creative Commons

http://www.creativecommons.it/

Certificazione ISO/27001

https://en.wikipedia.org/wiki/ISO/IEC_27001:2013

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

Deve essere confermata ogni anno.

I controlli presenti nell'Annex A rappresentano un'ottima checklist per iniziare.

Parte di una famiglia di standard più ampia
https://en.wikipedia.org/wiki/ISO/IEC_27000-series

Certificazioni

NIST Framework

https://www.nist.gov/cyberframework
National Institute of Standards and Technology (NIST), agenzia USA per la promozione di innovazione e competitività.

The Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

Certificazioni

ISA/IEC 62443

(ex ISA99)
Per indirizzare i temi di information security in contesti come quello dell'automazione industriale.
ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

Questo e altri standard qui:
https://en.wikipedia.org/wiki/Cyber_security_standards

Gestione e sicurezza

Gestione e sicurezza

Senza gestione non può esserci sicurezza.

Come faccio a definire delle policy di sicurezza aziendali se non conosco ruoli, funzioni, necessità ecc. degli utenti ?

Il perimetro aziendale a volte è complesso (partecipate, consociate, consulenti, insourcing, outsourcing ecc.).

Nessuna tecnologia può aiutarmi a sapere “chi fa che cosa” in azienda.

Serve organizzazione, metodo, policy e profonda conoscenza del proprio “environment”.

A volte bisogna comunque arrivare a soluzioni di compromesso.

Separazione delle funzioni

Ripensare organigrammi e funzioni in modo da separare le funzioni.
Evitare la presenza di conflitti di interesse e situazioni di controllore e controllato nella stessa linea gerarchica.
Classico esempio: chi implementa sicurezza diverso da chi la verifica.
Responsabile sicurezza riporto molto alto nella scala gerarchica (richiesto dal GDPR).
Più facile utilizzando servizi in outsourcing.

Gestione dei processi IT

Gestione dei processi IT