Cosa dobbiamo fare per difendere i nostri dati e rispettare il nuovo Regolamento Europeo?

ING. MAURIZIO SQUAIELLA

Senior Consultant di Top Management Consulting

GDPR: Tavola Sinottica Normativa

Top Management Consulting

Rispetto Art. 5:
-Trattati in modo lecito, corretto e trasparente
-Finalità determinate, esplicite, legittime
-Minimizzazione (dati adeguati, pertinenti, limitati)
-Dati esatti e se necessario aggiornati -> procedure per darne garanzia (es. cancellazione o rettifica)
-Conservati non oltre il conseguimento delle finalità
-Garanzia misure di sicurezza nel trattamento (integrità, disponibilità, riservatezza)

Criteri di Liceità e Condizioni per il Consenso al trattamento (Art. 6, 7,8,9) -> onere del titolare dimostrarlo

Riscontro diritti interessati – Art.12-22 – accesso (15), oblio/cancellazione (17), portabilità (20), opposizione (21)

Art. 25: Privacy by Design e by Default

Nomina DPO

Analisi rischi e DPIA

Regolamentazione dei rapporti con soggetti esterni o outsourcer

Registro dei trattamenti

ACCOUNTABILITY

pseudonimizzazione o cifratura

contromisure per **garantire** riservatezza, integrità, disponibilità (vedi analisi rischio in quanto sono i principi cardine della sicurezza informatica) → **assessment IT**

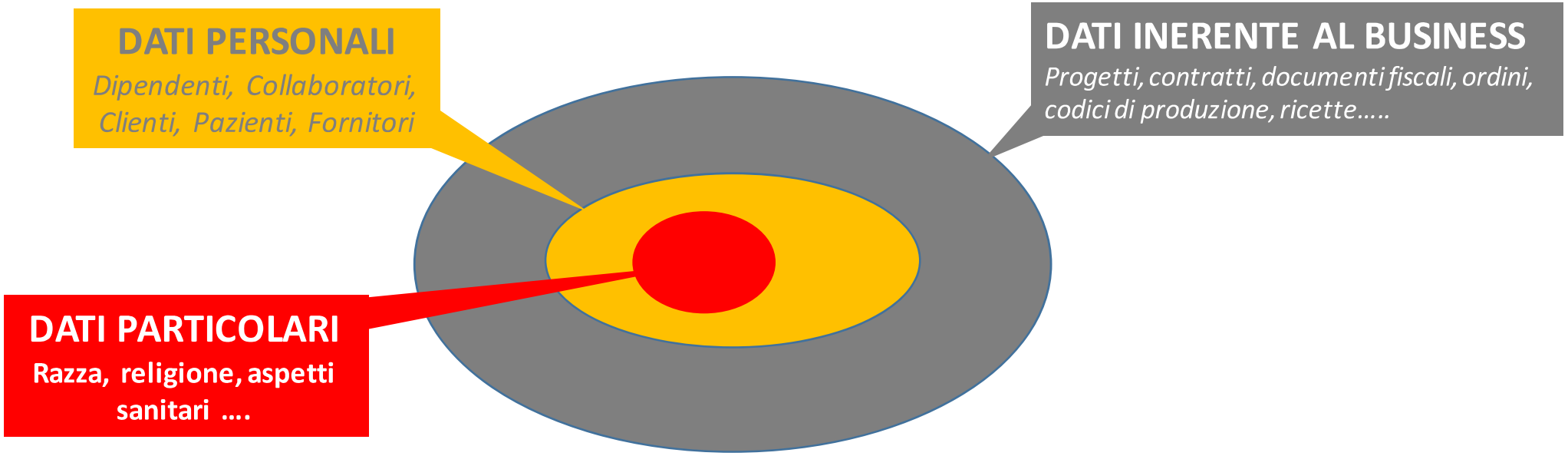
ripristino disponibilità e accesso dati → disaster recovery (procedure organizzative e contromisure con soluzioni informatiche, strumenti di incident response)

procedure per test, verifica e valutazione efficacia delle misure tecniche e organizzative → Procedure/policies, strumenti e soluzioni per l'Audit sicurezza e IT (penetration test, sw analisi log, ecc.)

Art. 32: Misure adeguate

7 PASSI PER UN'ADEGUATA DIFESA

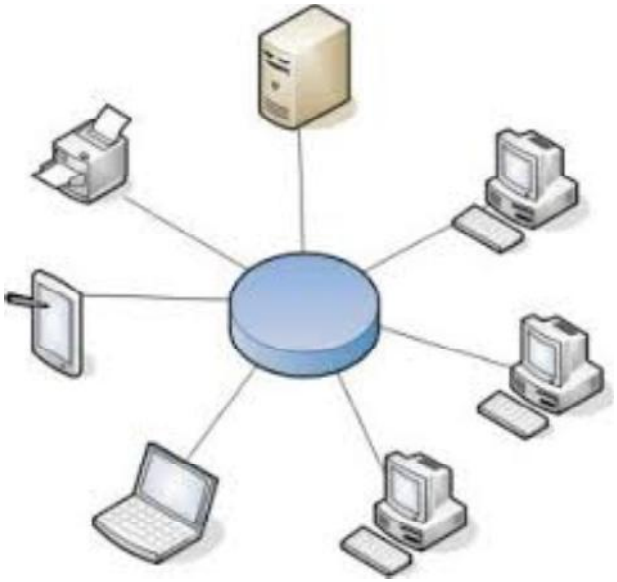
1. IDENTIFICARE BENE QUALI DATI DEVO DIFENDERE



TMC
Top Management Consulting

7 PASSI PER UN'ADEGUATA DIFESA

2. IDENTIFICARE BENE DOVE SONO I DATI DA DIFENDERE



Il Regolamento Europeo N.679/2016: Principi Generali

TRASPARENZA

- Adottare informative alternative, ad es. fatte di simboli o icone, e fruibili anche online o da smartphone
- È intesa anche verso l'interno dell'organizzazione del titolare del trattamento (ad es. tra gli autorizzati del trattamento)
- L'informativa deve essere anche concisa, intellegibile, facilmente accessibile

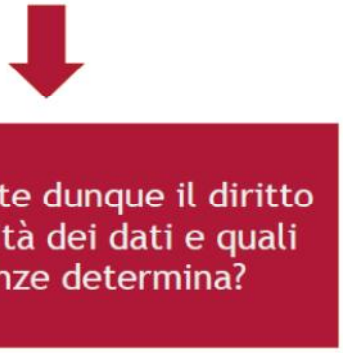
DIRITTI DELL'INTERESSATO

Art. 20 Diritto alla portabilità dei dati

L'interessato ha il diritto di ricevere in un formato **strutturato, di uso comune e leggibile a macchina** i dati personali che lo riguardano, che siano stati forniti ad un titolare del trattamento e **ha il diritto di trasmettere tali dati ad un altro titolare**, senza impedimenti da parte del primo, qualora:

a) il trattamento si basi sul consenso o su un contratto
e
b) il trattamento sia effettuato con mezzi automatizzati.

Esempi: trasferimento del c/c bancario con le transazioni degli ultimi 10 anni



DIRITTI DELL'INTERESSATO

Art. 20 Diritto alla portabilità dei dati

- Formato strutturato, di uso comune e leggibile a macchina = requisiti minimi per **l'interoperabilità**
- Non comporta l'obbligo di conservare i dati oltre il periodo previsto e strettamente necessario
- Il titolare deve garantire una sicurezza appropriata ai dati personali (trattamenti non autorizzati o illegali, eventuali perdite accidentali), e quindi **predisporre misure tecniche e organizzative contro la distruzione o il danneggiamento**
- Prevedere il **tracciamento nei sistemi** per capire se si tratta di dati potenzialmente soggetti al diritto della portabilità
- Selezionare le **informazioni che si possono o meno trasferire** (es. dati di altri interessati, o brevetti e proprietà intellettuale)

Art 30 Registri delle attività di trattamento

Ogni Titolare del trattamento nonché il suo rappresentante (**ndr: nonché gli eventuali responsabili ed eventuali DPO**) tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale documentazione contiene le seguenti informazioni **MINIME**:

- il nome e i dettagli del Titolare del trattamento, dei Responsabili, del DPO;
- la finalità del trattamento;
- una descrizione delle categorie di interessati e dei dati personali;
- le categorie di soggetti ai quali i dati personali sono stati o saranno comunicati;
- se applicabile, il trasferimento dei dati a Paesi terzi o ad organizzazioni internazionali, includendo l'identificazione di tali Paesi o organizzazioni;
- se previsti, i limiti temporali per la cancellazione di differenti categorie di dati;
- se possibile, una descrizione generale delle misure tecniche e organizzative per la sicurezza dei dati.

Art 30 Registri delle attività di trattamento

Occorre ricordare che il comma V dell'Art. 30 esonera dall'obbligo di tenuta del registro le aziende con meno di 250 dipendenti, a meno che:

- il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato;
- il trattamento non sia occasionale;
- vengano trattati categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

... CIO' NONSTANTE È FORTEMENTE CONSIGLIATO REDIGERLO UGUALMENTE

Top Management Consulting

Il Regolamento Europeo N. 679/2016: Registri delle attività di trattamento

Il registro dei trattamenti risponde infatti ad una pluralità di finalità, in quanto:

- È volto a tenere traccia delle operazioni di trattamento effettuate all'interno della singola organizzazione;
- costituisce uno **strumento operativo di lavoro** mediante il quale censire in maniera ordinata le banche dati e gli altri elementi rilevanti per assicurare un sano «ciclo di gestione» dei dati personali;
- rappresenta un **documento probatorio** mediante il quale il Titolare del trattamento può dimostrare di aver adempiuto alle prescrizioni del Regolamento, nell'ottica del principio di *accountability*.

… occorre ricordare che non esiste una regola generale che stabilisca le modalità attraverso le quali costruire il registro dei trattamenti **… ragion per cui è consigliabile aggiungere informazioni ulteriori rispetto quelle minime obbligatorie…**

ADEMPIMENTI FORMALI:
IL REGISTRO DEI TRATTAMENTI (art. 30)

INFORMAZIONE MINIME

Attività di trattamento	Titolare/Responsabile	Finalità	Descrizione categorie di interessati e dati personali	Categorie di destinatari	Eventuale trasferimento dei dati a paesi terzi	Termini ultimi per la cancellazione dei dati	Descrizione delle misure di sicurezza adottate ex art. 32
gestione amministrativa personale dipendente: rilevazione presenze tramite APP	xy spa	rilevazione presenze	dipendenti e collaboratori		holding xy presso stabilimento USA	in base alla normativa per la gestione LUL	APP conformi (segnalazione attivazione GPS, informativa privacy, consenso al trattamento)

INFORMAZIONI AGGIUNTIVE

Attività di trattamento	Dato particolare	L'attività principale comporta prevede che il Dato particolare sia trattato su vasta scala	Rischio elevato per i diritti e le libertà fondamentali	L'attività principale comporta il monitoraggio regolare e sistematico su larga scala degli interessati	Trattamento automatizzato (es. profilazione)	Sorveglianza su larga scala di zona accessibile al pubblico
Es. gestione amministrativa personale dipendente – rilievi presenze	SI (geolocalizzazione)	SI	SI	NO	NO	NO

ANALISI DEL RISCHIO - MISURA DEGLI IMPATTI

ISO/IEC 29134

LEVEL OF IMPACT	DESCRIPTION
Low	Gli interessati possono incontrare alcuni piccoli inconvenienti superabili senza particolari problemi (perdita di tempo per re-inserimento di dati, fastidi, irritazioni, ecc.).
Medium	Gli interessati possono incontrare notevoli inconvenienti superabili con qualche difficoltà (costi extra, impossibilità temporanea di accesso ai servizi di business, di preoccupazioni e timori ed incomprensioni, stress, minori fastidi fisici, ecc.).
High	Gli interessati possono incontrare notevoli conseguenze superabili solo anche se con gravi difficoltà (appropriazione indebita di fondi, blacklist da istituzioni finanziarie, i danni alla proprietà, la perdita di occupazione, citazione in giudizio, il peggioramento della salute, ecc.).
Very high	Gli interessati possono incontrare proplemi significativi, o anche conseguenze irreversibili e non superabili (incapacità di lavorare a lungo termine psicologico o disturbi fisici, morte, ecc.).

ANALISI DEL RISCHIO – VALUTAZIONE CONTESTO

Top Management Consulting

KEYMAP

CONTESTO

Quale forma giuridica ha la Società?

srl

Di che tipo è la proprietà della Società?

Privata

La Società è controllata da soggetti terzi?

No

La Società è quotata in borsa?

No

La società possiede marchi o brevetti?

No

In quale settore opera la Società?

Raffinerie, prodotti chimici, gomma, plastica, industrie farmaceutiche

Qual è la tipologia dei Clienti della Società?

Aziende Nazionali, Aziende Internazionali

La Società opera negli USA o Canada?

No

Numero Dipendenti

18

Numero Collaboratori a contratto

18

Fatturato anno precedente (MLN?)

1,1

Fatturato previsto anno in corso (MLN?)

1,2

Struttura di vendita

Diretta

Numero Anagrafiche Clienti, Dipendenti, Collaboratori e Fornitori gestite nei sistemi azie

AMMINISTRAZIONE SISTEMA INFORMATIVO

Il ruolo di Amministratore di sistema è stato documentato ed attribuito in modo
lo ricoprono?

No

Le utenze privilegiate da Amministratore sono distinte da quelle non privile
Registrano i file di log? Sono assegnate ognuna a una specifica persona?

Parzialmente

Prima di collegare un nuovo dispositivo alla rete sono sostituite le credenziali
un amministratore autorizzato?

No

Sono stati identificati e documentati i profili e le autorizzazioni per accedere
sicurezza delle informazioni?

Parzialmente

Esiste un sistema per la registrazione, profilazione degli utenti e la gest
opportuna politica degli accessi?

Si

Esiste un sistema per impedire che vengano utilizzate credenziali deboli,
sufficiente frequenza e ne venga impedito il riutilizzo?

Parzialmente

Sono stati identificati, classificati e registrati le applicazioni e i programmi s
delle informazioni trattate?

No

Sono stati identificate le applicazioni ed i programmi software, con le relati
dispositivo (whitelist)?

No

KEYMAP

KEYMAP

POSTA ELETTRONICA

Come è gestita la posta elettronica?

Su un mail server interno

Sono sempre utilizzati ed aggiornati i programmi di Antispam?

Si, quasi sempre

ORGANIZZAZIONE PER LA SICUREZZA DELLE INFORMAZIONI

La Società possiede la certificazione ISO9001 o analoga per lo specifico settore di appartenenza?

Si

La Società possiede la certificazione ISO27001?

No

Esiste un organigramma aziendale?

Si

Le mansioni, i ruoli e le responsabilità sono identificate, documentate ed attribuite in modo specifico?

Si

Esistono procedure documentate per la gestione della sicurezza dei dati?

Parzialmente

Il rispetto delle procedure e la loro efficacia è periodicamente verificato?

Parzialmente

Le procedure e le responsabilità per la sicurezza dei dati sono state opportunamente ed esplicitamente spiegate ai dipendenti e ai collaboratori?

Parzialmente

Il personale interno ed esterno è stato addestrato sui rischi che possono insorgere durante la manipolazione e trattamento dei dati?

Parzialmente

Nelle lettere di assunzione e/o nelle mansioni sottoscritte dal personale esistono vincoli specifici inerenti alla sicurezza e riservatezza delle informazioni? Ed in particolare, se trattate, per le informazioni personali o particolari?

Si

DATI PERSONALI E PARTICOLARI

La Società tratta dati personali o particolari?

ANALISI DEL RISCHIO
VALUTAZIONE DEL RISCHIO SPECIFICO

		Livello di impatto		
		Basso	Medio	Alto / Molto alto
Probabilità di occorrenza di un evento	Bassa			
	Media			
	Alta			

RISCHIO SPECIFICO – CONTROMISURE IDONEE

Misure tecniche di sicurezza

	Dispositivi mobili / portatili	
Q.1	Deve essere definita e documentata una procedura di gestione pei dispositivi mobili e portatili che definisce regole chiare per il loro corretto utilizzo.	1
Q.2	I dispositivi mobili che accedono al sistema informativo devono essere pre-registrati e pre-autorizzati.	1
Q.3	I dispositivi portatili devono essere soggetti agli stessi livelli di procedure di controllo di accesso (al sistema informativo) della altre apparecchiature.	1
Q.4	Devono essere chiaramente definite specifiche responsabilità e ruoli per la gestione dei dispositivi mobili.	2
Q.5	L'organizzazione deve essere in grado di cancellare da remoto i dati personali (associati al suo utilizzo) su un dispositivo mobile la cui sicurezza sia stata messa a repentaglio.	2
Q.6	I dispositivi mobili devono consentire la separazione tra utilizzo personale e aziendale attraverso contenitori software sicuri.	2
Q.7	I dispositivi portatili, quando non in uso, devono essere fisicamente protetti contro il furto.	2
Q.8	Per l'accesso ai dispositivi mobili devono venir prese in considerazione tecniche di autenticazione a due fattori	3
Q.9	I dati personali memorizzati in un dispositivo mobile (utilizzato per l'elaborazione di dati aziendali) devono essere cifrati.	3
	Correlati a ISO 27001:2013 - A. 6.2 i dispositivi mobili e il telelavoro	

RISCHIO SPECIFICO – CONTROMISURE IDONEE

Misure tecniche di sicurezza

	Risorse umane	
	Riservatezza del personale	
I.1	L'organizzazione deve assicurare che tutti i dipendenti comprendano le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità devono essere chiaramente comunicati durante la fase di pre-impiego e/o del processo di inserimento.	1
I.2	Ai dipendenti deve essere chiesto preventivamente di esaminare e accettare la politica di sicurezza dell'organizzazione e di firmare i relativi accordi di riservatezza e di non divulgazione.	2
I.3	I dipendenti coinvolti in trattamenti di dati personali ad alto rischio devono essere legati a specifiche clausole di riservatezza (tramite il contratto di lavoro o altro atto giuridico).	3
	Correlati a ISO 27001:2013 - A.7 Sicurezza delle risorse umane	

ADEMPIMENTI SOSTANZIALI: I PROCESSI VALUTATIVI

Se Dipendenti > 250 o trattamento comporta rischio elevato o comprende dati particolari	Registro trattamenti (art.30)
Se il Titolare è un ente pubblico o tratta dati particolari su larga scala, ecc.	DPO (art. 37)
Se il trattamento comporta un rischio elevato…	DPIA (analisi del rischio con contenuti minimi prefissati) – Art. 35
Se DPIA evidenzia un rischio elevato senza misure di attenuazione in campo	Consultazione preventiva (art. 36)
Livello di sicurezza adeguato al rischio	Analisi del rischio → Misure di sicurezza adeguate **(art. 32), che prevedano, se del caso:**

pseudononimizzazione o cifratura

contromisure **per garantire** riservatezza, integrità, disponibilità (vedi analisi rischio in quanto sono i principi cardine della sicurezza informatica) → dal punto di vista IT comporta l'esigenza di effettuare **un assessment IT**

ripristino disponibilità e accesso dati → disaster recovery (procedure organizzative e contromisure con soluzioni informatiche, strumenti di incident response,)

procedure per test**, verifica e valutazione efficacia delle misure tecniche e organizzative** → Procedure/policies, strumenti e soluzioni per **l'Audit sicurezza e IT (penetration test, sw analisi log, ecc.)**

TMC
Top Management Consulting

7 PASSI PER UN'ADEGUATA DIFESA

4. AGGIORNARE ED AFFILARE LE ARMI

Non a caso si parla di attacco informatico
perché si tratta di una vera e propria guerra ed in guerra
le armi sono importanti.

Armi che sono sempre più sofisticate e tecnologiche

7 PASSI PER UN'ADEGUATA DIFESA

Il nostro modo di lavorare si è evoluto ….

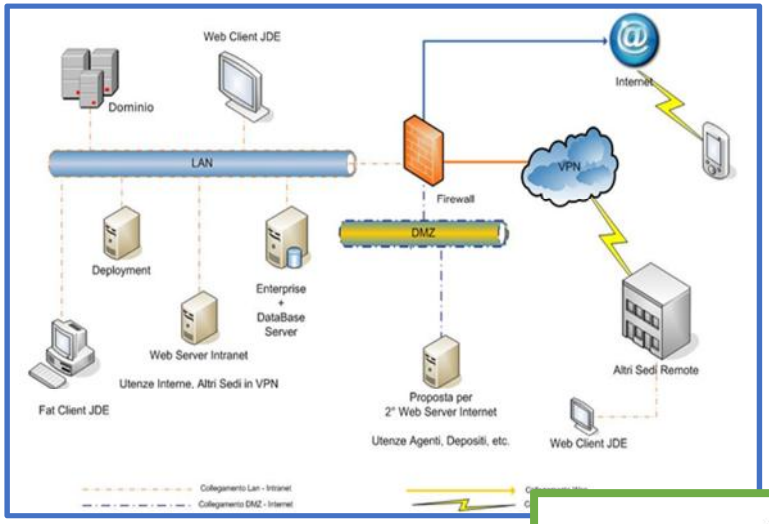
…..e le «armi» necessarie per difendere il nostro business sono molte, diverse e sempre più evolute e sofisticate

NON POSSIAMO PERMETTERCI DI IGNORARLO!!

Net Intrusion Detection System → Firewall → Anti virus → Anti spyware → Backup e disaster recovery → Software di Emulazione terminali → Intrusion Detection System → Protezione Wi-fi → Criptazione → SW sentinella

7 PASSI PER UN'ADEGUATA DIFESA

5. ADEGUARE LE INFRASTRUTTURE



Oggi i dati sono nei server dell'Azienda,
e nei dispositivi mobile dei dipendenti

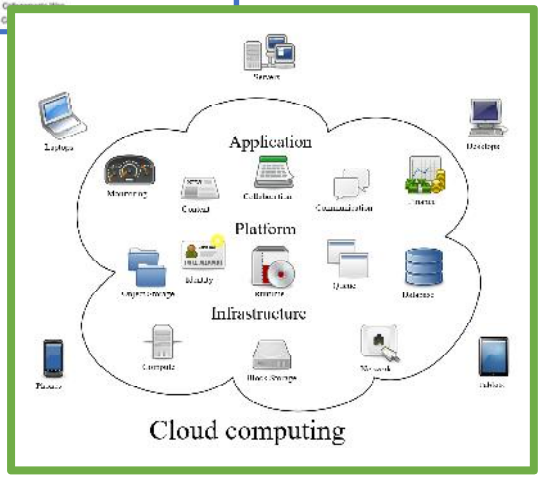
Fuori ci sono i virus che attaccano gli internauti
ed i loro mobile (end point)

E gli eserciti di hacker che attaccano i server
con tempo e risorse infinite

La possibilità di salvarsi dipende, oltre che dalle tecnonologie adottate (le armi), da come sono progettate le infrastrutture del sistema informatico aziendale (le difese):

- Segmentazione delle reti;
- Policy di accesso dall'esterno;
- Disaster recovery;
- Sistemi evoluti di document management
- Gestione pw e autorizzazioni
- Zone protette

…… Cloud computing



TMC
Top Management Consulting

10 CONSIGLI UTILI

1. Installate un buon Antivirus , tenetelo costantemente aggiornato e usatelo su tutti i file che ricevete.
2. Fate il backup (almeno) dei vostri dati. Fatelo spesso. Fatelo SEMPRE
3. Installate gli aggiornamenti (patch) di Microsoft .
4. Non installate software superfluo o di dubbia provenienza.
5. Non aprite gli allegati non attesi, di qualunque tipo, chiunque ne sia il mittente, e comunque non apriteli subito, anche se l'antivirus li dichiara ''puliti''.
6. Tenete disattivati ActiveX , Javascript e Visual Basic Scripting . Riattivateli soltanto quando visitate siti di indubbia reputazione.
7. Non fidatevi dei link presenti nei messaggi di posta. Possono essere falsi e portarvi a un sito-truffa.
8. Non inviate posta in formato html e chiedete di non mandarvela
9. Non distribuite documenti word : trasportano virus e contengono vostri dati personali nascosti.
10. Per aumentare la sicurezza del browser è spesso consigliato togliere la memorizzazione automatica dei moduli e delle password .

7 PASSI PER UN'ADEGUATA DIFESA

6. DEFINIRE LE PROCEDURE DI DIFESA

Questo, ci «obbliga»

- *ad analizzare bene i processi aziendali ed a descriverli in modo chiaro e comprensibile*
- *a valutare le minacce, i rischi e gli eventuali danni*
- *a definire ed evolvere le strategie di protezione e difesa*
- *a definire e documentare le procedure*

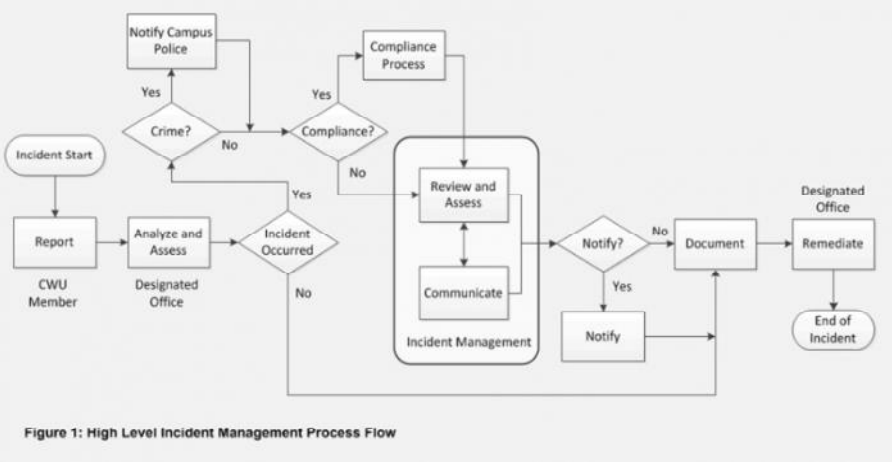


Figure 1: High Level Incident Management Process Flow

TMC
Top Management Consulting

7 PASSI PER UN'ADEGUATA DIFESA

… in ogni tempo ed in ogni guerra, oltre alle armi ed alle strutture di difesa, quello che ha sempre fatto la differenza è stato …

… l'organizzazione, l'addestramento e la disciplina dei soldati!!!!

7 PASSI PER UN'ADEGUATA DIFESA

7. ADDESTRAMENTO CONTINUO DEL PERSONALE

Questo, ci «aiuta»

- *creare consapevolezza sui possibili rischi*
- *creare competenza sulle procedure da utilizzare*
- *Diminuire la distanza tra «praticità d'uso» e sicurezza*

PER FAR SÌ CHE OGNI PERSONA SAPPIA DISCIPLINARE E CONTROLLARE I PROPRI COMPORTAMENTI PER DIFENDERSI DALLE MINACCE E REAGIRE IN CASO DI ATTACCO

ALCUNI DATI 2017

36,2% FALLE NEL CODICE DEI SOFTWARE AZIENDALI
24,5% COMPORTAMENTO DEGLI UTENTI
20,8% STRUMENTI DI SICUREZZA OBSOLETI

Fonte: Rapporto Osservatorio Attacchi Digitali in Italia 2017. Pubblicato il 18/05/2017.

TMC
Top Management Consulting

In quale percentuale i dipendenti o i collaboratori interni sono, in modo colposo o doloso, coinvolti in crimini o danni informatici a scapito della propria azienda?

100%

TMC
Top Management Consulting

10 CONSIGLI UTILI PER APPROCCIARE LA NUOVA PRIVACY

1. Tutti i soggetti che trattano i dati devono **ricevere una lettera di incarico**
2. Se la gestione dei dati è affidata a società terze, bisogna **nominare i Responsabili Esterni**
3. E' opportuno che l'azienda predisponga e consegni un **Disciplinare per l'utilizzo degli strumenti informatici agli incaricati**
4. Il sito internet aziendale deve **rispettare la normativa sui cookies**
5. **L'installazione di telecamere** in azienda prevede informative e previa approvazione
6. **Le buste paga** devono essere gestite tutelando i dati dei dipendenti
7. Per utilizzare strumenti informatici bisogna adottare 3 misure minime: **password, antivirus e firewall**
8. **L'aggiornamento** dei sistemi operativi e degli altri software installati è obbligatorio
9. **Marketing e geolocalizzazione**: raccolta e utilizzo dei dati devono essere gestiti con cura
10. Gli incaricati al trattamento dati devono **essere formati**

TMC
Top Management Consulting

Cosa dobbiamo fare per difenderci e limitare i costi di un possibile attacco informatico?

Adeguare e tenere aggiornate le tecnologie

Formare ed addestrare il personale

Riprogettare le infrastrutture

Adeguare gli aspetti contrattuali

Adeguare le procedure ed i comportamenti alle norme di riferimento ed alle best practise del mercato

NEMMENO IL VOSTRO ANGELO CUSTODE SA DA DOVE INIZIARE?