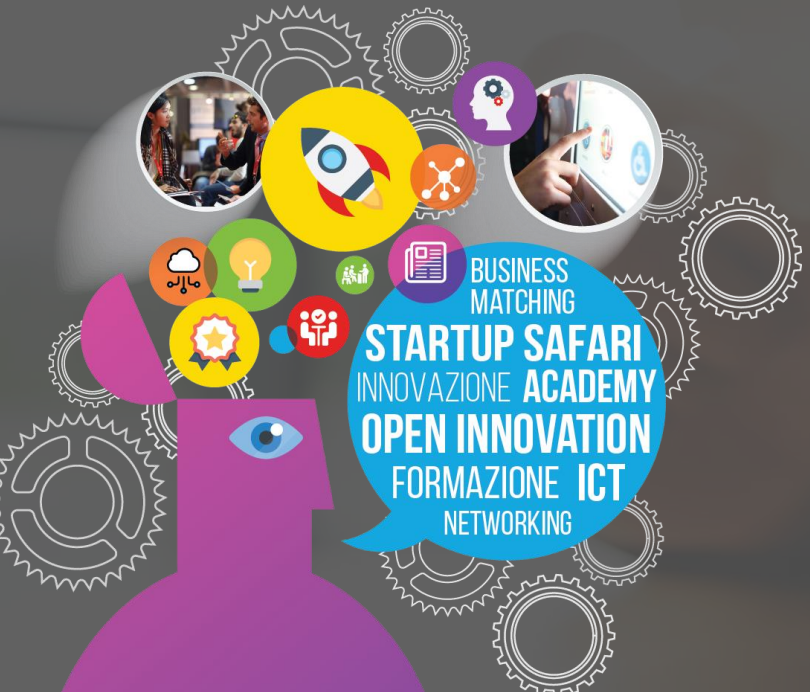
smau

PADOVA FIERE

PADOVA

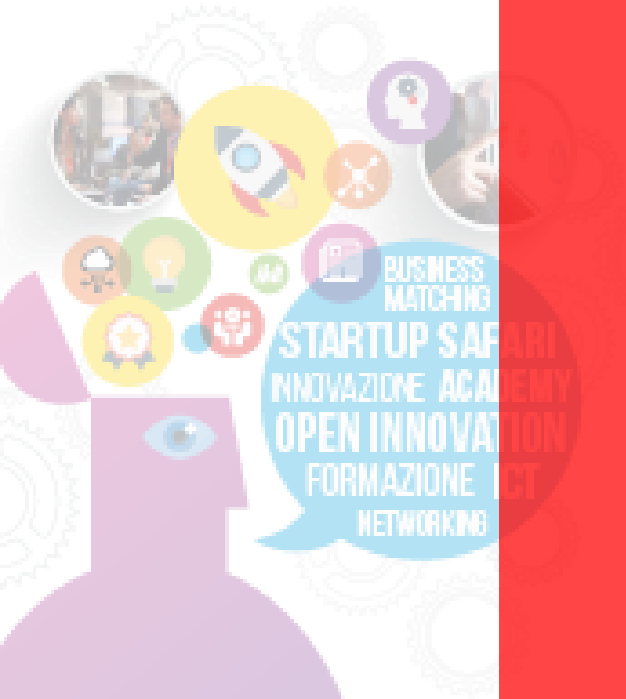
22-23 MARZO 2018



GDPR e Cyber Security: approccio multidimensionale

smau
PADOVA 22-23 MARZO 2018

PADOVA FIERE



Agenda

- Executive summary
- Contesto di riferimento
- Roadmap di attuazione
- Cosa è cambiato
- Cosa accade in caso di violazioni dei dati
- Quali misure tecnologiche adottare
- 2016 principali attacchi e maggiore vulnerabilità
- Come approcciare la vulnerabilità del fattore cultura generale

smau
PADOVA 22-23 MARZO 2018

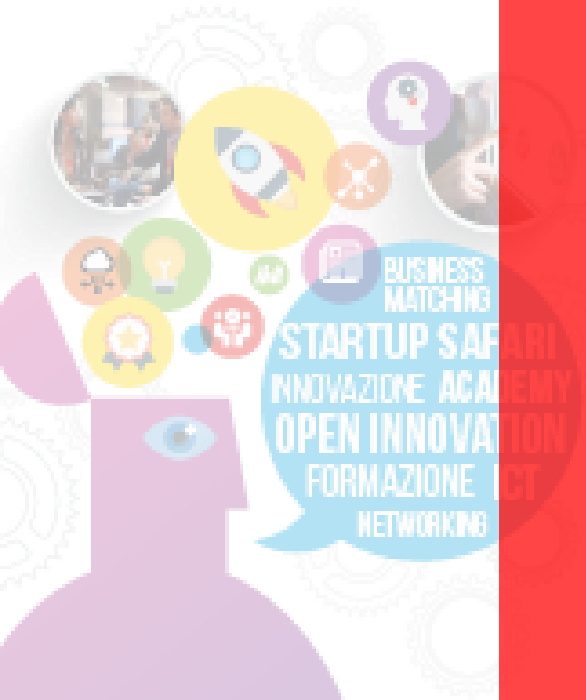
PADOVA FIERE

AIPSI - www.aipsi.org (www.aipsi.org)

- **AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, capitolo Italiano** di **ISSA**, Information Systems Security Association, (**www.issa.org**) **che conta** >>10.000 Soci, la più grande associazione non-profit di professionisti della Sicurezza ICT nel mondo
- **AIPSI è il punto di aggregazione sul territorio e di trasferimento di know-how per i professionisti della sicurezza digitale, sia dipendenti sia liberi professionisti ed imprenditori del settore**
- **Sede Centrale:** Milano
- **Sedi territoriali** : Ancona-Macerata, Lecce, Torino, Verona-Venezia
- **Contatti**: aipsi@aipsi.org, segreteria@aipsi.org

smau
PADOVA 22-23 MARZO 2018

PADOVA FIERE



Primari obiettivi AIPSI

Aiutare i propri Soci nella **crescita professionale** e quindi nella crescita del loro business

offrire ai propri Soci **servizi qualificati** per tale crescita, che includono

Convegni, workshop, webinar sia a livello nazionale che internazionale via ISSA

Rapporti annuali e specifici OAD, Osservatorio attacchi Digitali in Italia

Supporto nell'intero ciclo di vita professionale

Formazione specializzata e supporto alle certificazioni, in particolare eCF Plus (EN 16234-1:2016, in Italia UNI 11506)

Rapporti con altri soci a livello nazionale (AIPSI) ed internazionali (ISSA)

Contribuire alla diffusione della cultura e la sensibilizzazione per la sicurezza informatica agli utenti digitali

Collaborazione con varie Associazioni ed Enti per eventi ed iniziative congiunte: AICA, Assintel, Assolombarda, Anorc, CSA Italy, FidaInform, FTI, Inforav, Polizia Postale, Smau, i vari ClubTI sul territorio, ecc.

OAD
Osservatorio
Attacchi Digitali
in Italia

smau
PADOVA 22-23 MARZO 2018

PADOVA FIERE

OAD, Osservatorio Attacchi Digitali in Italia (ex OAI)

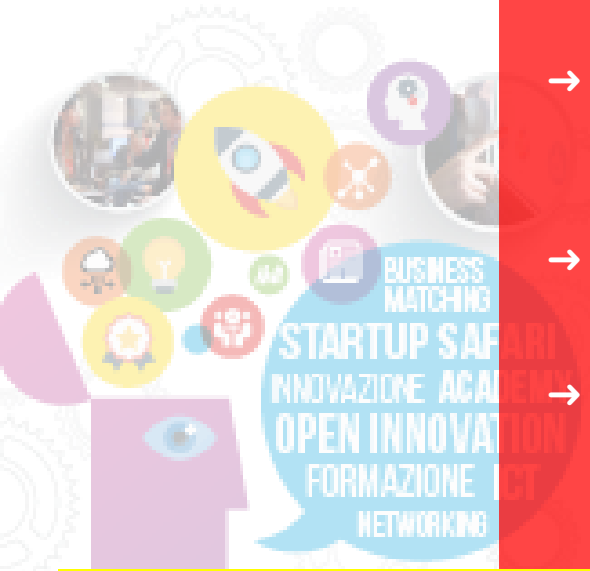
OAD Osservatorio Attacchi Digitali in Italia

- ***Che cosa è***
  - Indagine via web sugli attacchi digitali intenzionali ai sistemi informatici in Italia

→ ***Obiettivi iniziativa***
- Fornire informazioni sulla reale situazione degli attacchi digitali in Italia
- Contribuire alla creazione di una cultura della sicurezza informatica in Italia, sensibilizzando in particolare i vertici delle aziende/enti ed i decisori sulla sicurezza informatica

→ ***Che cosa fa***
- Indagine generale annuale e specifiche su argomenti caldi, condotte attraverso un questionario on-line indirizzato a CIO, CISO, CSO, ai proprietari/CEO per le piccole aziende

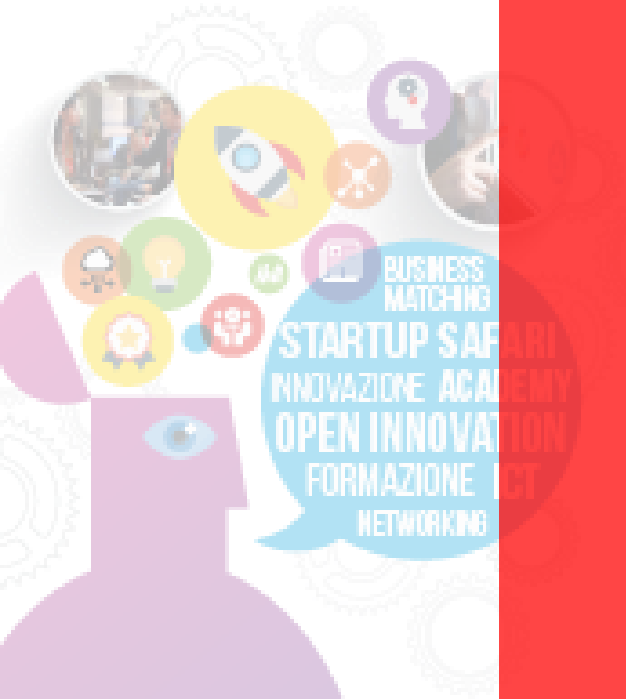
→ ***Come***
- Rigore, trasparenza, correttezza, assoluta indipendenza (anche dagli Sponsor)
- Rigoroso anonimato per i rispondenti ai questionari
- Collaborazione con numerose Associazioni (Patrocinatori) per ampliare il bacino dei rispondenti e dei lettori



Tutti i Rapporti OAD (e OAI) pubblicati dal 2008 ad oggi sono scaricabili gratuitamente da https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/precedenti-rapporti-oad-oai.html

smau
PADOVA 22-23 MARZO 2018

PADOVA FIERE



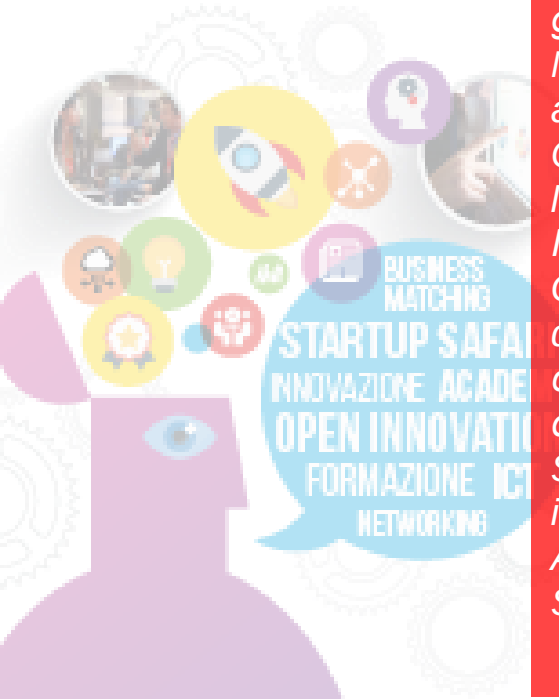
Chi è Fine Tuning

Fine Tuning Consulenza Integrata è società di consulenza ed un system integrator specializzato nella fornitura di servizi professionali altamente qualificati e nella progettazione di soluzioni cross-market innovativi. In ambito sicurezza offre:

- Consulenza tecnica e organizzativa sulle normative di riferimento
- Check Up ed assesment sulla security del perimetro digitale aziendale
- Formazione specialistica rivolta ad utenti con diverso livello di competenza
- Privacy compliance: Log Collection e Privileged Activity Monitoring
- Progettazione di infrastrutture custom e integrazione di soluzioni di mercato

smau
PADOVA 22-23 MARZO 2018

PADOVA FIERE



LUCA BONADIMANI

Luca Bonadimani, socio AIPSI e responsabile per l'area Nord-Est, laurea e master di II livello in Filosofia, master in gestione aziendale. inizia la sua carriera occupandosi di ICT nel settore editoriale per diversi anni, per poi gestire per un breve periodo l'ufficio comunicazione di Gardaland S.p.A.
Nel 1996 fonda con un socio Fine Tuning Consulenza Integrata, web solution agency di Verona. Seguono altre sue iniziative imprenditoriali quali BSZ Communication, finetuning.it, Xtrategy, nonché l'ambizioso progetto Talete per la vendita on line di libri a tiratura limitata.
Nel 2000 avviene l'incontro con GEA Consulenti Associati e la fondazione di Gea Lab, società di consulenza e-business. Nello stesso anno riceve l'incarico di dirigere come Amministratore Delegato la neo-nata Adria Lab, web solution company partecipata dall'allora Merloni Elettrodomestici, Gea Lab e dall'Università degli Studi di Ancona.
Successivamente dirige prima ed amministra poi Nesting Scrl, società di innovazione tecnologica con soci il Cefriel e la Fondazione di Venezia. Oggi è Amministratore della società da lui fondata: Fine Tuning Consulenza Integrata Srl.

Contesto di riferimento

CONTESTO

Ad aprile 2016 il Parlamento Europeo ha approvato il nuovo **Regolamento generale sulla protezione dei dati**, il quale introduce numerose novità relative ai diritti degli interessati, ai criteri di conformità, alle modalità di controllo e alle sanzioni da applicare in caso di violazione.

DESTINATARI DEL REGOLAMENTO

Sono soggetti all'applicazione del Regolamento tutti gli enti pubblici e le imprese che trattano dati classificati (sensibili, biometrici, sanitari, giudiziari, etc) e/o che raccolgono grandi quantità di dati personali.

Contesto di riferimento

SOLUZIONI PROPOSTE

Di seguito si propone l'applicazione delle migliori soluzioni per garantire il rispetto dei requisiti tecnici, quali la gestione ed il monitoraggio degli accessi alle informazioni, la cifratura dei dischi e dei file e la gestione delle informazioni in mobilità.

VANTAGGI PER IL CLIENTE

Il rispetto del Regolamento e l'adozione delle soluzioni proposte consente di **mitigare le conseguenze di un eventuale *data breach*** e soprattutto **evitare perdite finanziarie** dirette (sanzioni da versare all'autorità di controllo) e indirette (danni alla reputazione, perdita di fiducia e rispetto da parte dei clienti, etc).

Contesto di riferimento

NORMATIVA PRE-ESISTENTE

La direttiva 95/46/CE[1] – fulcro della normativa UE in materia di protezione dei dati personali – è stata introdotta nel 1995 con due obiettivi: salvaguardare il diritto dei cittadini alla protezione dei dati e garantire la libera circolazione dei dati personali tra gli Stati membri.

L'ESIGENZA DI CAMBIARE

Gli sviluppi tecnologici hanno completamente modificato il contesto di riferimento: la tecnologia attuale consente alle imprese private così come agli enti pubblici di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività.

[1] Testo integrale della Direttiva 95/46/CE

Contesto di riferimento

LA NUOVA NORMATIVA

Il 27 aprile 2016, dopo un iter legislativo durato più di 4 anni e comprendente circa 4mila emendamenti, il Parlamento Europeo ha approvato il nuovo **Regolamento generale sulla protezione dei dati**[2] che abroga la direttiva 95/46/CE e dovrà essere adottato entro il 25 maggio 2018.

OBIETTIVI

Il rispetto del Regolamento e l'adozione delle soluzioni proposte consente di **mitigare le conseguenze di un eventuale *data breach*** e soprattutto **evitare perdite finanziarie** dirette (sanzioni da versare all'autorità di controllo) e indirette (danni alla reputazione, perdita di fiducia e rispetto da parte dei clienti, etc).

[2] Testo integrale del Regolamento (UE) 2016/679

Roadmap di attuazione

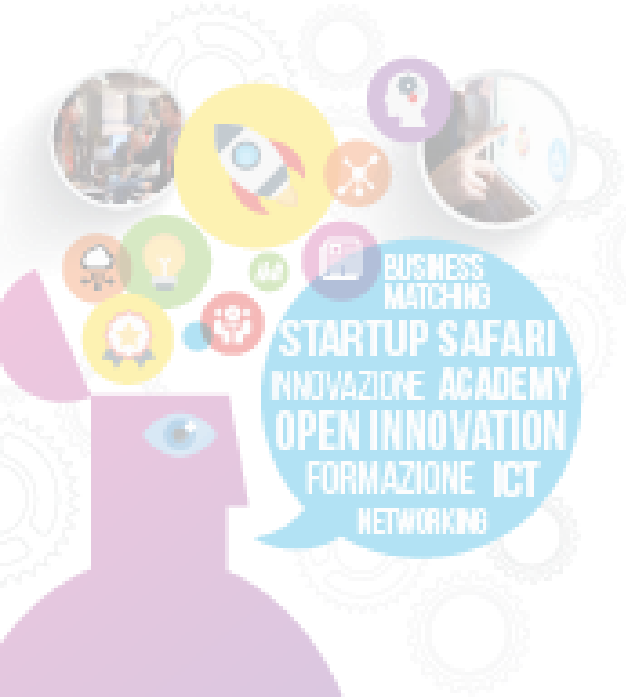
✔ **27 Apr 2016 Approvazione**
Il Parlamento Europeo ha approvato la versione definitiva del Regolamento.

✔ **04 Mag 2016 Divulgazione**
Il Regolamento UE 2016/679 è stato pubblicato nella Gazzetta Ufficiale Europea.

✔ **25 Mag 2016 Entrata in vigore**
Il Regolamento UE 2016/679 è ufficialmente entrato in vigore. Gli Stati membri hanno due anni di transizione per istituire le autorità di controllo nazionali ed adeguare le normative locali.

🏁 **25 Mag 2018 Termine per l'adozione da parte degli Stati membri**
Entro tale data dovranno essere attuate tutte le disposizioni già previste dalla legge e dalle future integrazioni ancora da emettere.

Cos’è cambiato



Le principali differenze tra la direttiva del ’95 – recepita e integrata dalla normativa italiana con il D.Lgs. 196/2003 e successive integrazioni – ed il nuovo Regolamento riguardano principalmente tre macro-aree:

Figure di riferimento
Consenso
Sanzioni

Cos'è cambiato

	Direttiva 95/46/CE	Regolamento UE 2016/679
Figure di riferimento	• Incaricato • Responsabile del trattamento	• Incaricato • Responsabile del trattamento • **Responsabile della protezione dei dati (Data Protection Officer)**
Consenso	Qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento.	Il consenso deve essere espresso **esplicitamente** mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano. Qualora il trattamento abbia più finalità, il **consenso deve essere prestato per tutte queste.**
Sanzioni	Gli Stati membri adottano misure appropriate per garantire la piena applicazione delle disposizioni della direttiva e stabiliscono le sanzioni da applicare in caso di violazione delle disposizioni della stessa.	Sono previste sanzioni molto severe per coloro che violano le norme sulla protezione dei dati: **fino a 20 milioni € o al 4% del loro fatturato globale annuo** (tale valore varierà in funzione della natura, della gravità e della durata della violazione, del carattere doloso o colposo dell'illecito, etc).

smau
PADOVA 22-23 MARZO 2018

PADOVA FIERE

Cosa accade in caso di violazione dei dati

Avvenuta violazione (data breach)

L'Autorità Garante adotterà una serie di provvedimenti che prevedranno l'obbligo di comunicare i casi in cui - a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi - si dovesse verificare la perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o trattati.

Cosa accade in caso di violazione dei dati

Avvenuta violazione (data breach) → **Notifica all'Autorità Garante**

L'Autorità Garante adotterà una serie di provvedimenti che prevedranno l'obbligo di comunicare i casi in cui - a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi - si dovesse verificare la perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o trattati.

Il responsabile del trattamento sarà tenuto ad avvisare l'Autorità Garante dell'avvenuta violazione dei dati senza ritardo - dove possibile entro 72 ore - dal momento della scoperta della violazione stessa.
In caso di ritardo, la notifica dovrà essere corredata da una giustificazione documentata.

Cosa accade in caso di violazione dei dati

Avvenuta violazione (data breach) → Notifica all'Autorità Garante → **Notifica all'interessato**

L'Autorità Garante adotterà una serie di provvedimenti che prevedranno l'obbligo di comunicare i casi in cui - a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi - si dovesse verificare la perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o trattati.

Il responsabile del trattamento sarà tenuto ad avvisare l'Autorità Garante dell'avvenuta violazione dei dati senza ritardo - dove possibile entro 72 ore - dal momento della scoperta della violazione stessa.
In caso di ritardo, la notifica dovrà essere corredata da una giustificazione documentata.

Il responsabile del trattamento sarà tenuto ad avvisare anche l'interessato dell'eventuale violazione dei suoi dati personali (*data breach notification*).

Cosa accade in caso di violazione dei dati

L'Autorità Garante adotterà una serie di provvedimenti che prevedranno l'obbligo di comunicare i casi in cui - a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi - si dovesse verificare la perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o trattati.

Il responsabile del trattamento sarà tenuto ad avvisare l'Autorità Garante dell'avvenuta violazione dei dati senza ritardo - dove possibile entro 72 ore - dal momento della scoperta della violazione stessa.
In caso di ritardo, la notifica dovrà essere corredata da una giustificazione documentata.

Il responsabile del trattamento sarà tenuto ad avvisare anche l'interessato dell'eventuale violazione dei suoi dati personali (*data breach notification*).

L'eventuale sanzione dovrà essere efficace, proporzionata e dissuasiva. L'ammontare sarà fissato tenendo conto della natura, della gravità e della durata della violazione, del carattere doloso o colposo dell'illecito. L'Autorità propone **sanzioni pecuniarie fino a 20 milioni € o al 4% del fatturato globale annuo**.

Cronache di guerra 2016: le vittime

Dall'inizio del 2016 la criminalità informatica ha avuto un impatto diretto su:

Vita politica

Banche

Trasporti

Istituzioni

… e numerose altre aree critiche della nostra società.

Cronache di guerra 2016: l'Italia

> *"Over confidence is a slow and insidious killer"*

Valore totale del mercato IT.....**66 Mld€**

Spesa totale per la sicurezza.....**1 Mld€**

che rapportata al nostro PIL equivale a **0,05%**

Cronache di guerra 2016: minacce n°1

Ransomware

Va a segno nel **3%** dei casi

Nel 2016 marca **+120%** rispetto al 2015

Phishing

Da più di **20** anni sulla cresta dell'onda

Nel 2016 ha causato **2,3 Mld€** di danni

Conclusioni dai primi 10 attacchi

Il **60%** degli attacchi è causato dal **fattore umano**

Inconsapevolezza, imperizia, imprudenza, dolo, negligenza

Conclusioni dai primi 10 attacchi

> *“The reason people continue to be the weakest link is that most organizations continue to fail to invest in them”*

Lance Spitzner, training director c/o SANS Securing the Human Program

smau
PADOVA 22-23 MARZO 2018

PADOVA FIERE

Come difendersi?

FORMAZIONE

TECNOLOGIA

COMPLIANCE

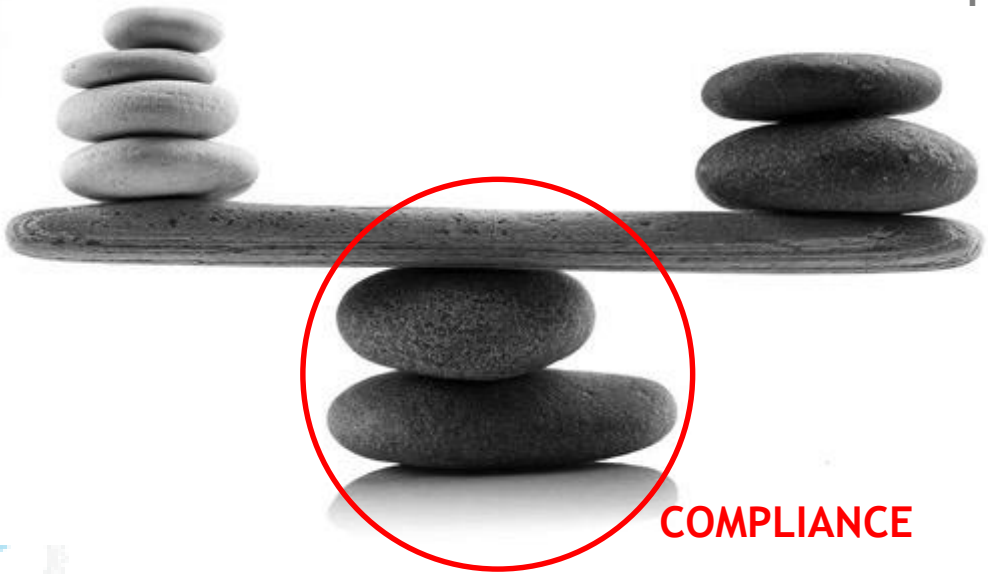
smau
PADOVA 22-23 MARZO 2018

PADOVA FIERE

Come difendersi?

FORMAZIONE

TECNOLOGIA



COMPLIANCE

Contesto di riferimento

Dobbiamo smettere di vivere le normative e le best practice internazionali come un obbligo.
L'adozione di metodologie e processi affidabili è la base su cui costruire il business.

General Data Protection Regulation

- Ha l'obiettivo di proteggere i dati personali dei cittadini europei
- Si rivolge indistintamente a PA e aziende private
- Impone adeguamenti organizzativi e tecnici

Network and Information Security Directive

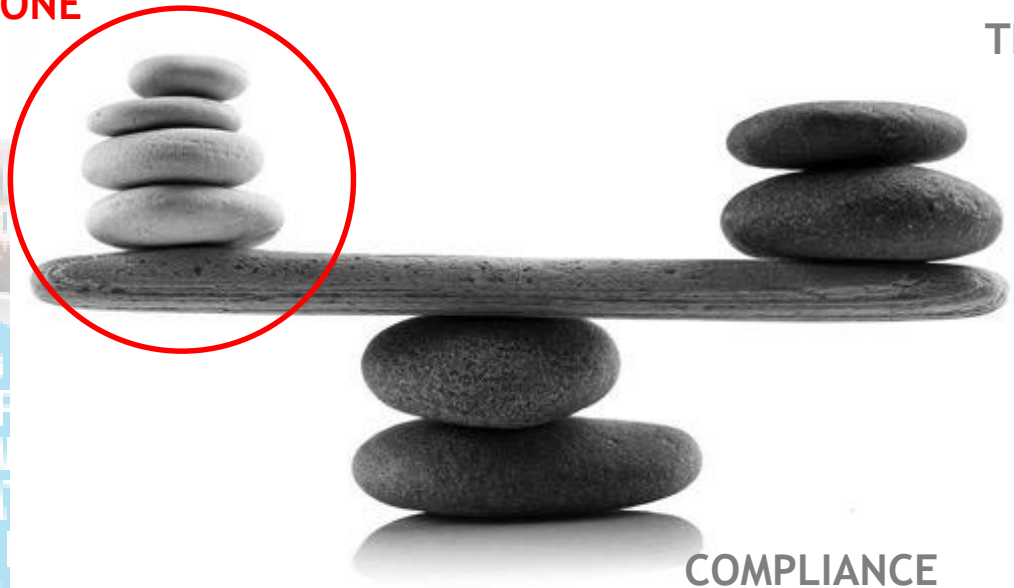
- Ha l'obiettivo di proteggere le infrastrutture critiche degli stati membri
- Si rivolge ad operatori dei servizi essenziali e fornitori di servizi digitali
- Impone la definizione di strategie nazionali di cyber security

smau
PADOVA 22-23 MARZO 2018

PADOVA FIERE

Come difendersi?

FORMAZIONE



TECNOLOGIA

COMPLIANCE

Formazione dell'organizzazione

L'offerta formativa si sta specializzando su corsi specifici legati al recepimento organizzativo del GDP, sotto un esempio di pacchetti

TITOLO	MODALITÀ	LIVELLO	DESTINATARI	DURATA
Misure minime sicurezza informatica	FAD	Base	End-user	2h
Il Regolamento europeo per la protezione dei dati (GDPR) e sua applicazione	FAD	Base	Addetti al trattamento	4h
Il Regolamento europeo per la protezione dei dati (GDPR): le novità rispetto al D.lgs 196/2003	FAD	Base	Addetti al trattamento	4h
Metodologie e principali standard di sicurezza	FAD	Base	Addetti al trattamento	4h
Risk Management	FAD + Aula	Intermediate	Responsabili del trattamento	8h
Sicurezza delle informazioni: incident handling	FAD + Aula	Intermediate	Operatori della sicurezza	8h

smau
PADOVA 22-23 MARZO 2018

PADOVA FIERE

Formazione dell'organizzazione

Modalità di fruizione

E-learning
compatibile anche con smartphone e tablet

In aula
con un docente qualificato

Ibrida
con teoria a distanza ed esercitazioni in aula

Da richiedere

Account di supervisione
per monitorare lo stato di avanzamento degli utenti

Esami
intermedi e finali per la verifica delle competenze

Attestato finale
di partecipazione e superamento

Destinatari ticipi

Impiegati
Per l'acquisizione delle competenze di base

Tecnici
Per l'aggiornamento delle competenze specialistiche

Manager
Per comprendere le normative e gli standard

Cosa accade in caso di violazione dei dati

Gestione e monitoraggio degli accessi

Definizione delle policy per l'accesso alle informazioni e la data loss prevention e monitoraggio proattivo delle attività privilegiate degli amministratori IT.

Full-disk encryption

Cifratura dei dischi locali delle postazioni di lavoro fisse o mobili che contengono dati classificati o consentono l'accesso ad essi.

File encryption

Cifratura dei singoli file contenenti dati classificati a prescindere dalla loro posizione – dischi locali, share di rete, dischi rimovibili – e dal dispositivo utilizzato (desktop, smartphone, tablet).

Gestione delle informazioni in mobilità

Controllo dei dispositivi mobile – smartphone e tablet – aziendali e privati e gestione dei contenuti classificati scambiati mediante la posta aziendale o i servizi di cloud storage.

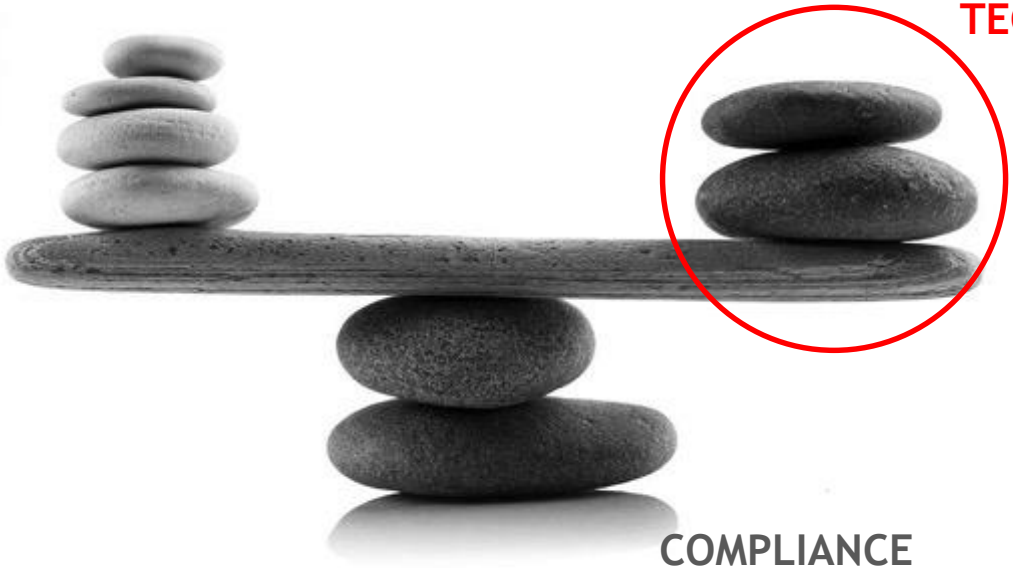
smau
PADOVA 22-23 MARZO 2018

PADOVA FIERE

Come difendersi?

FORMAZIONE

TECNOLOGIA



COMPLIANCE

Cosa accade in caso di violazione dei dati

"E se mi rubassero dei dati cifrati?"

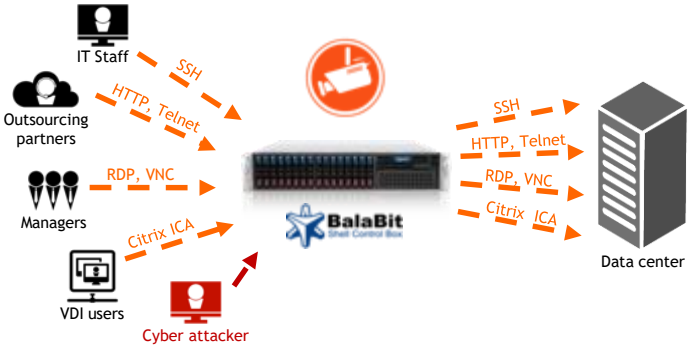
Se il Data Protection Officer è in grado di dimostrare che i dati sottratti erano cifrati si può evitare la notifica dell'avvenuto data breach agli interessati e, previa valutazione dell'Autorità di controllo, non si incapperà in sanzioni amministrative.

Cosa accade in caso di violazione dei dati

Privileged Activity Monitoring: BalaBit Shell Control Box

Lo Shell Control Box è uno strumento che effettua il monitoraggio e l'audit degli accessi amministrativi remoti diretti a uno o più server mediante il controllo delle connessioni in chiaro o crittografate.

Si tratta di uno strumento indipendente dai client e dai server che opera in rete come *man-in-the-middle* e pertanto non richiede alcuna modifica delle applicazioni esistenti.

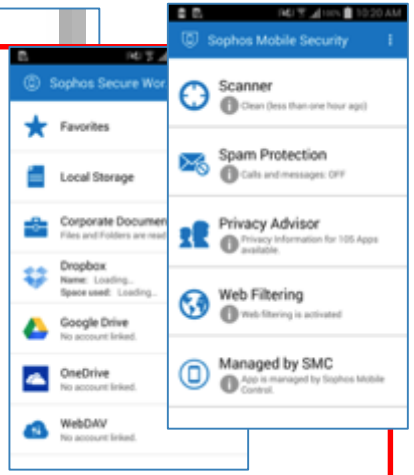


Le sessioni testuali (es. SSH e Telnet) o grafiche (es. RDP, Citrix ICA, VNC) sono salvate in file legalmente inoppugnabili crittografati e firmati con timestamp. Gli *audit trail* includono il filmato corredato dei comandi in input e della scansione del testo mostrato a schermo.

Cosa accade in caso di violazione dei dati

Enterprise Mobility Management: Sophos Mobile Control

Il Mobile Control è una piattaforma compatibile con smartphone e tablet **iOS, Android e Windows Phone/Mobile**, che include le funzionalità di MDM (Mobile Device Management), MAM (Mobile Application Management) e MCM (Mobile Content Management).



Tra le principali funzionalità troviamo la gestione della compliance dei dispositivi (aziendali e privati), il controllo delle app installate, il blocco, la localizzazione e la cancellazione remota nonché l'accesso sicuro alle risorse aziendali (es. posta e cartelle condivise).

La recente integrazione con il SafeGuard Enterprise garantisce l'accesso sicuro ai documenti cifrati senza rischiare che la perdita o il furto del dispositivo compromettano la confidenzialità dei dati.

Cosa accade in caso di violazione dei dati

Encryption: Sophos SafeGuard Enterprise

Sophos SafeGuard è una suite di cifratura modulare che include gli endpoint per Windows e Mac ed una console centralizzata per la gestione del ciclo di vita delle chiavi.

SafeGuard supporta nativamente la **cifratura del disco di boot** mediante l'integrazione con BitLocker di Microsoft e FileVault 2 di Apple.

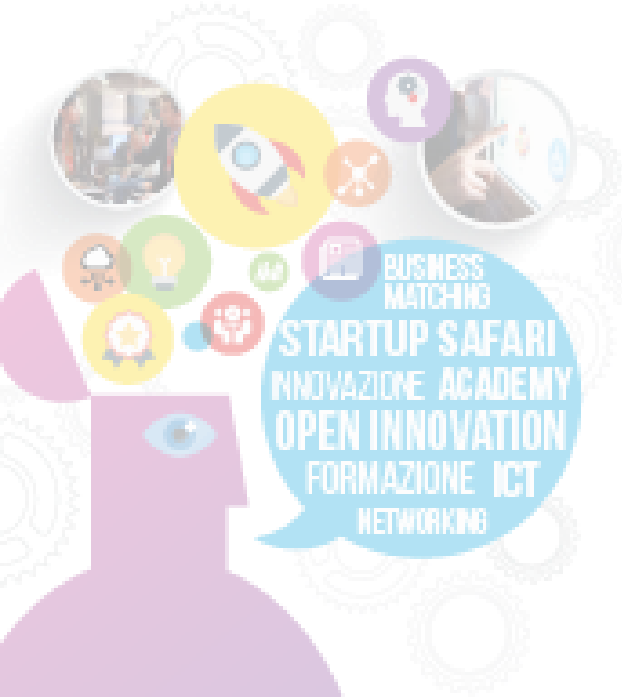
SafeGuard supporta inoltre la **cifratura dei file locali e condivisi** mediante network share, dispositivi rimovibili, terminali mobili, cloud storage e posta elettronica.

Il processo di cifratura, modifica e condivisione dei file è del tutto trasparente per l'utente che dispone delle opportune autorizzazioni. Qualunque accesso ai dati è invece precluso ai non autorizzati.

smau
PADOVA 22-23 MARZO 2018

PADOVA FIERE

AIPSI



Grazie per l'attenzione.

Volete approfondire l'argomento?

Venite a trovarci.