aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

ISSA
Information Systems Security Association

seeweb

11 Aprile 2018 – SeewebAcademy

GDPR e sicurezza digitale
Alcune considerazioni pratiche

Marco R. A. Bozzetti

Presidente AIPSI
CEO Malabo srl

AIPSI ed i suoi primari obiettivi https://www.aipsi.org/

- **AIPSI, Associazione Italiana Professionisti Sicurezza Informatica,** è **capitolo Italiano** di **ISSA**, Information Systems Security Association, (**www.issa.org**) **che conta** >>10.000 Soci nel mondo, la più grande associazione non-profit di professionisti della Sicurezza ICT
- **AIPSI è il punto di aggregazione sul territorio e di trasferimento di know-how per tutte le persone che a vario titolo e livello si occupano professionalmente della sicurezza digitale, sia come dipendenti sia come liberi professionisti ed imprenditori del settore**
- **Primari obiettivi AIPSI**
  - Aiutare i propri Soci nella **crescita professionale** e quindi nella crescita del loro business

Fornire supporto nell'intero ciclo di vita professionale, creando anche contatti tra i Soci AIPSI e con quelli ISSA

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

- Convegni e webinar sia a livello nazionale che internazionale via ISSA
- ISSA Journal mensile
- Rapporti nazionali e internazionali, tra cui OAD, Osservatorio attacchi Digitali in Italia
- Formazione specializzata
- Supporto alle certificazioni, in particolare eCF Plus (EN 16234-1:2016, in Italia UNI 11506)

Le principali novità di AIPSI

- Nuovo sito web dell' Associazione: https://www.aipsi.org
- Nuovo sito web per OAD: https://www.oadweb.it
- Sedi territoriali AIPSI: Macerata, Venezia, Verona, Torino
- Accordo con AICA per promuove le certificazioni eCF sulle competenze della sicurezza digitale
- Supporto al CSCL, Cyber Security Career Lifecycle
- Azioni in corso per essere riconosciuti dal MISE, Ministero Sviluppo Economico, entro la fine del 2018 come Associazione rappresentativa dei professionisti della sicurezza digitale secondo la Legge 4/2013
- Webinar asincroni e sincroni
- Nuovo Media Partner: Reportec

OAD, Osservatorio Attacchi Digitali in Italia

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

- ***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**

OAD
Osservatorio
Attacchi Digitali
in Italia

2008 - 2018 : 10 anni di indagini via web

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

OAD
Osservatorio
Attacchi Digitali
in Italia

Tutti i Rapporti OAD (e OAI) pubblicati dal 2008 ad oggi sono scaricabili gratuitamente dal sito OAD e da quello AIPSI

Questionario OAD 2018: da compilare subito!

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

https://www.oadweb.it/limesurvey/index.php/661199

Assolutamente anonimo, risposte predefinite tra cui scegliere, rapido da compilare con il salto automatico di domande non pertinenti, include domande su attacchi a *sistemi di automazione industriale, IoT, blockchain*

Come ringraziamento a chi completa il Questionario la possibilità di scaricare gratuitamente:

- **ISSA Journal di Gennaio 2018 con i migliori articoli del 2017**
- **Il volume (in pdf) di Reportec " ICT Security e Data Protection 2017"**

ISSA
Information Systems Security Association International

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

GDPR
e
Sicurezza digitale

GDPR: ma *mi* servi?

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

- Così come per le precedenti norme sulle privacy, Il GDPR costituisce un forte fattore di leva per il potenziamento e miglioramento delle misure di sicurezza digitale tecniche ed organizzative, che sono sempre più necessarie INDIPENDENTEMENTE dalla privacy per la CONTINUITA' OPERATIVA dell'Azienda/Ente

- MA, analogamente alle precedenti norme, adempiere effettivamente al GDPR, è UN IMPEGNO SERIO non può e non deve essere presso alla leggera, date anche le pesanti sanzioni economiche. Da ben 22 anni (del 1996 la prima legge sulla privacy) dovrebbero essere attive e gestite le idonee misure di protezione dei dati personali, e quindi anche della sicurezza digitale, con le ovvie evoluzioni che si sarebbero dovute apportare nel corso di tutti questi anni

- Ma le strutture organizzative piccole e piccolissime, che sono la stragrande maggioranza nella realtà italiana hanno la voglia di approcciare seriamente privacy e sicurezza digitale?

  - Ho ben altri seri problemi cui pensare e dedicare il mio tempo!
  - Ho ben altre spese cui far fronte !
  - La privacy è solo inutile burocrazia: che dati confidenziali vuoi che abbia?
  - Forti sanzioni? Ma quando mai verranno a controllarmi?
  - Sicurezza digitale? Ho già l'antivirus e il controllo degli accessi … Il resto è troppo complicato e costoso e poi chi mai vorrà attaccarmi digitalmente?

GDPR: ma quanto *mi* costi?

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

La privacy richiede da sempre un effettivo e sostanziale coinvolgimento del vertice dell'Azienda/Ente e di Responsabili interni, sia nella fase preparatoria, sia in quella di gestione periodica e continua

Può essere necessario il ricorso a preparati e seri consulenti esterni, oltre all'eventuale DPO

Almeno 50 tipi di documenti (per strutture medio-piccole), alcuni dei quali *working*, che includono:

- **Registro dei trattamenti**
- **Analisi rischi ed impatti**
- **Elenco autorizzati e Responsabili (sia interni che di Terze Parti), con relative lettere di incarico**
- **Gestione delle Terze Parti cui si terziarizza tutto o parte di un trattamento**
- **Struttura e procedure organizzative**
- **Strumenti informatici di supporto e misure di sicurezza digitale per la protezione dei dati personali**

- **GDPR lascia alla responsabilità del Titolare l'individuazione delle idonee misure di sicurezza digitale, a seguito dell'Analisi dei rischi, ma evidenzia la necessità/opportunità di criptare i dati personali, e di individuare data breach**

I *cattivi* Consiglieri …e Fornitori …

- **Per il GDPR**
  - Numerosi consulenti , commercialisti avvocati, fornitori ICT offrono servizi «chiavi in mano» a prezzi ridicoli, che non possono che offrire soluzioni e documenti generali e non contestualizzati sulla realtà del Cliente
  - Tali soluzioni costitusicono una minima copertura o sono soldfi mal spesi, anche se pochi?
- **Per la sicurezza digitale**
  - Con un analogo approccio, molti fornitori di ICT vendono le soluzioni che hanno, trascurando le effettive necessità del Cliente ed approfittando della sua incompetenza

I principali strumenti di difesa per la sicurezza digitale

- *di prevenzione e protezione*
  - Crittografia, Stenografia
  - Periodiche analisi del rischio vs pr
  - Si
  - ar
  - Si
  - Id
  - au
  - (LD
  - An
  - Co
  - Sicu
  - Arc
- *di ripri*
  - Back
  - Disas
- *di gesti*
  - Tecnic
  - Organizzativa: formazione e addestramento, operation (ITIL v3), help-desk/contact center, ERT, ..

inio

re, …)

• da approccio reattivo a proattivo

• contestualizzare misure tecniche ed organizzative alla propria realtà

• Analisi dei rischi e degli impatti

• approccio architetturale ben bilanciato

• riferimento ai principali standard e alle best practices ben consolidate: OSA, ITIL v3, Cobit, ISO 27000, NIST SP, …

nteraggio, verifica SLA, gestione delle patch e delle release del software (→ licenze)

L'evoluzione delle misure di sicurezza digitale …

- **Le misure di sicurezza digitale evolvono con l'evolversi degli attacchi e della loro complessità.**
- **Le «tradizion… ma non sufficienti a c…ati attacchi**
- **Nuove tecnic…**
  - Sistemat… di *intellige…*c.
  - **Scanner…**ni e di dati
  - **Correlaz…**li eventi
  - **Tecniche euristiche** per "problem solving"
  - **Evoluzione algoritmi di crittografia: curve ellittiche, crittografia quantistica (viene usato un canale di comunicazione segreto basato sullo scambio di fotoni polarizzati su fibra ottica)**

Ruolo crescente dell'intelligenza artificiale (AI) nella sicurezza digitale

Prime conclusioni ….

- **Il GDPR forse (??) non sarà una bomba atomica, ma richiede un impegno serio e continuo, e quindi dei costi diretti ed indiretti**
- **La sicurezza digitale è ormai un MUST per qualsiasi attività e business, dato che è determinante per la continuità operativa dell'Azienda/Ente. E' indipendente dalla privacy, ma ne è un elemento fondamentale**
- **GDPR e sicurezza digitale hanno dei costi non trascurabili, ma quali sono i costi della «non privacy» e della «non sicurezza»?**
- **Di questi tempi tutti si vendono come esperti di privacy e di sicurezza digitale .. sono i pochi business che tirano per ora .. Ma come si fa discernere tra i millantatori ed i professionisti seri, soprattutto per decisori non esperti dei temi? Un suggerimento (condizione necessaria ma non sufficiente): verificare per la persona:**
  - **Una o più certificazioni sulla privacy e sulla sicurezza digitale , in particolare quelle con valore legale europeo: eCF - EN 16234 1:2016**
  - **l'appartenenza ad una o più associazioni professionali esistenti in Italia per la privacy e la sicurezza digitale**

In ritardo rispetto alla scadenza ?

- **In ritardo rispetto alla scadenza del 25/5/2018?**
- **NESSUN PANICO: stendere un Piano di Lavoro con ragionevoli scadenze per interventi da effettuare anche dopo tale data.**
- **Per gli interventi a breve, meglio se entro maggio-giugno 2018 e tutti da documentare (inversione dell'onere della prova!):**
  - **A livello organizzativo:**
    - **Registro dei Trattamenti**
    - **Nomina dei Responsabili e degli autorizzati**
    - **Analisi rischi ed impatti**
    - **Informativa interessati e loro consenso esplicito**
  - **A livello tecnico**
    - **attivazione e/o miglioramento misure di base per la sicurezza digitale: controllo accessi, back-up e ripristino, anti malware, log di sistema e degli Amministratori**
    - **Misure fisiche di sicurezza per gli archivi cartacei**

ISSA
Information Systems Security Association International

https://www.issa.org/

https://www.aipsi.org/

marco.bozzetti@aipsi.org

Grazie per l'attenzione e ..

- **Visitate i siti web di AIPSI e OAD, e seguite i nostri eventi**
- **Iscrivetevi ad AIPSI-ISSA**
- **Compilate e fate compilare il Questionario OAD 2018**