Giancarlo Butti

SICUREZZA TOTALE 4.0

L'**ABC** sulla Physical Cyber Security per i **DPO** e le **PMI** (e non solo)

ITER®

Aggiornamenti su
www.iter.it/sicurezza

SICUREZZA TOTALE 4.0

L'ABC sulla Physical Cyber Security per i DPO e le PMI (e non solo)

di Giancarlo Butti

SICUREZZA TOTALE 4.0
L'ABC sulla Physical Cyber Security per i DPO e le PMI (e non solo)

Titolo originale prima edizione:

SICUREZZA TOTALE - Guida alla protezione dei beni aziendali

EDITORE

ITER Srl – Milano
Via A. Sacchini, 20
20131 Milano (MI)
www.iter.it

ISBN: 9788894441529

STAMPA

Digital book s.r.l.
Via Karl Marx, 9
06012 Cerbara - Città di Castello (PG)

Prima edizione marzo 2011

Seconda edizione settembre 2019

Copyright ITER Srl *(www.iter.it)*

Tutti i diritti sono riservati a norma di legge e a norma delle convenzioni internazionali.
Nessuna parte di questa pubblicazione può essere riprodotta con sistemi elettronici, meccanici o altri, senza l'autorizzazione scritta dell'editore.
Tutti i marchi citati sono registrati dai rispettivi proprietari.
Gli eventuali testi delle normative e di altri documenti riportati nel libro hanno solo finalità indicativa e non hanno alcun valore ufficiale.
Gli unici testi ufficiali delle normative sono quelli riportati sulla Gazzetta Ufficiale della Repubblica Italiana e Gazzetta ufficiale dell'Unione europea che prevalgono in caso di discordanza.

In ricordo
Dei miei Billy, Lord, Laika
Di Lassie, Lilli, Fata, Bea, Eden
Giancarlo

Un particolare ringraziamento
ad Alberto per la fattiva collaborazione,
a Gabriele, Paolo e Silvano
per le loro presentazioni e recensione

Giancarlo Butti *(giancarlo.butti@promo.it)*

(LA BS 7799), (LA ISO IEC 27001), CRISC, ISM, DPO, CBCI, AMBCI

Master in Gestione aziendale e Sviluppo Organizzativo (MIP - Politecnico di Milano).

Si occupa di ICT, organizzazione e normativa dai primi anni 80:

- analista di organizzazione, project manager, security manager ed auditor presso gruppi bancari
- consulente in ambito documentale, sicurezza, privacy… presso aziende di diversi settori e dimensioni.

Come divulgatore ha all'attivo:

- oltre 800 articoli su 30 diverse testate
- 23 fra libri e white paper, alcuni dei quali utilizzati come testi universitari
- 13 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT sulla sicurezza ICT in Italia
- relatore in oltre 120 eventi presso ABI, ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, TECNA…
- docente in master e corsi di perfezionamento post-universitario presso diversi atenei.

Socio di AIEA/ISACA (www.aiea.it – Associazione Italiana Information Systems Auditors), del CLUSIT (www.clusit.it – Associazione Italiana per la Sicurezza Informatica) e di BCI (Business Continuity Institute).

Partecipa ai gruppi di lavoro di ABI LAB, di ISACA-AIEA, di UNINFO, di Oracle Community for security…

Fra i coordinatori di www.europrivacy.info.

INDICE

PRESENTAZIONE DELLA SECONDA EDIZIONE ..... ***ix***
PRESENTAZIONE DI GABRIELE FAGGIOLI ix

PRESENTAZIONE DELLA PRIMA EDIZIONE ..... ***x***
PRESENTAZIONE DI PAOLO GIUDICE x
RECENSIONE DI SILVANO ONGETTA x

INTRODUZIONE ***1***
I CONTENUTI DEL LIBRO 2

PARTE PRIMA ***5***

GLI ASSET DA PROTEGGERE ***7***
GLI ASSET DAL PUNTO DI VISTA DELL'AZIENDA 7
I BENI MATERIALI 8
I BENI IMMATERIALI 9
LA CONOSCENZA 13
IL CAPITALE INTELLETTUALE 13
LA CLASSIFICAZIONE DELLE INFORMAZIONI 16
I DOCUMENTI 17
I DOCUMENTI ELETTRONICI 18
IL SISTEMA INFORMATIVO 19
IL CICLO DI VITA DELLE INFORMAZIONI 21
IL CAPITALE UMANO 23
ALTRI ASSET 25
METODOLOGIA ENISA PER LE PMI 26
LA COLLOCAZIONE DEI BENI AZIENDALI 27
LA VERIFICA DOCUMENTALE 27
GLI ASSET DAL PUNTO DI VISTA DELLA NORMATIVA PRIVACY 29
L'AMBITO DI TUTELA 29
I SOGGETTI TUTELATI 30

LA GESTIONE DEL RISCHIO ***33***
L'ANALISI DEL RISCHIO 33
I RISCHI 35
CORRELAZIONE FRA ASSET 36
LE MINACCE NEI CONFRONTI DEI BENI MATERIALI 37
LE MINACCE NEI CONFRONTI DEI BENI IMMATERIALI 38
EVENTI CORRELATI AL PERSONALE 40
I REQUISITI DI SICUREZZA 45
METODOLOGIA ENISA PER LE PMI 47
GLI IMPATTI PER L'AZIENDA 48
CORRELAZIONE FRA IMPATTI 48
LE MINACCE 52
MINACCE AMBIENTALI 52
MINACCE INDUSTRIALI 53
MINACCE – GUASTI 54
MINACCE COMPORTAMENTALI 55

LE VULNERABILITÀ 57
L'ANALISI DEI RISCHI DEL PUNTO DI VISTA DELL'AZIENDA 60
FASI DELL'ANALISI DEI RISCHI 60
ANALISI DEI RISCHI DAL PUNTO DI VISTA DEL GDPR 67
CONFRONTO FRA ANALISI DEL RISCHIO DAL PUNTO DI VISTA DELL'AZIENDA E DEL GDPR 76
TRATTAMENTO DEL RISCHIO 78
I COSTI DI RIPRISTINO 78
IL TRATTAMENTO DEL RISCHIO AZIENDALE 79
IL TRATTAMENTO DEL RISCHIO DAL PUNTO DI VISTA DEL GDPR 80
LA RILEVAZIONE DELLE MISURE DI SICUREZZA IN ATTO 80
L'ATTIVAZIONE DELLE CONTROMISURE 82
IL TRASFERIMENTO DEL RISCHIO 84
IL CICLO DELL'ANALISI DEL RISCHIO 85

LE MISURE DI SICUREZZA 87
CLASSIFICAZIONE DELLE MISURE DI SICUREZZA 87
CICLO DI VITA DELLE MISURE DI SICUREZZA 91
COERENZA NELLE CONTROMISURE 92
DIFFERENZA NELLE CONTROMISURE 94
ESEMPI DI MISURE DI SICUREZZA 96
MISURE DI CARATTERE GENERALE 97
RAPPORTI CON IL PERSONALE 98
GESTIONE DEGLI ACCESSI FISICI/LOGICI AGLI ASSET 99
RAPPORTI CON ESTERNI (FORNITORI/OUTSOURCER) 100
GESTIONE DELLA SICUREZZA 102
CONTROLLI 102
SICUREZZA FISICA 103
VIDEOSORVEGLIANZA 107
SICUREZZA LOGICA 108
GESTIONE DEI DOCUMENTI 118
LA CONTINUITÀ DEL BUSINESS 119
LE COMUNICAZIONI 122
CRITTOGRAFIA 126
PSEUDONIMIZZAZIONE 127
FIRME ELETTRONICHE 128
IMPLEMENTARE LE MISURE DI SICUREZZA 131
RIEPILOGO MISURE DI SICUREZZA BASE 131
CONTINUITÀ OPERATIVA 133
SICUREZZA FISICA 133

SCENARI OPERATIVI 135
TELEFONIA MOBILE 137
APPLICAZIONI END USER COMPUTING 138
SOCIAL MEDIA 140
LA GESTIONE DEI RIFIUTI ELETTRONICI 141
BIG DATA 143
BLOCKCHAIN E DLT 147

INTELLIGENZA ARTIFICIALE 149
CLOUD 153
IOT (INTERNET OF THINGS) 160

LE NORMATIVE SULLA SICUREZZA 165

LA PROTEZIONE DEI DATI PERSONALI E DEI DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE 167
LE MISURE DI SICUREZZA NEL D.LGS. 196/03 PRE GDPR 168
SEMPLIFICAZIONI 172
LE MISURE DI SICUREZZA NEL GDPR 176
I PROVVEDIMENTI CHE IMPATTANO LA SICUREZZA 179
LA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO 180
LA SICUREZZA DEGLI IMPIANTI 182
LA CRIMINALITÀ INFORMATICA 183
IL DIRITTO D'AUTORE 184
LA RESPONSABILITÀ AMMINISTRATIVA 186
CONTROLLI E LIMITI NEI CONTROLLI 187
I VINCOLI 187
LE SOLUZIONI 193
VADEMECUM PRIVACY E LAVORO - APRILE 2015 198
STRUMENTI UTILIZZATI DAL LAVORATORE PER RENDERE LA PRESTAZIONE LAVORATIVA 200
LA TUTELA DEL KNOW HOW 205

PARTE SECONDA - STRUMENTI OPERATIVI 207

MODULI PER LA RACCOLTA DI INFORMAZIONI 211
MISURE DI SICUREZZA DELLA SEDE 213
MISURE DI SICUREZZA DEI LOCALI 215
MISURE DI SICUREZZA DEL CED 217
ARCHIVI CARTACEI (DOCUMENTI / SUPPORTI) 219
RILEVAZIONE DELLE COMPETENZE/CONOSCENZE 230
STRUMENTI PER MAPPARE PROCESSI E TRATTAMENTI 233
LA RILEVAZIONE DEI PROCESSI AZIENDALI 233
SCHEDE DI RILEVAZIONE DI UN PROCESSO 235
LA RILEVAZIONE DEI FLUSSI DOCUMENTALI 238
IL DPS COME STRUMENTO DI MAPPATURA 241
ESEMPI DI POLICY E PROCEDURE 249
ESEMPIO 1 - CLASSIFICAZIONE DEI DATI PERSONALI/INFORMAZIONI 250
ESEMPIO 2 - NORME DI COMPORTAMENTO 252
ESEMPIO 3 - REGOLE PER LE COMUNICAZIONI AZIENDALI DA E VERSO L'ESTERNO 260
ESEMPIO 4 - POLICY PER L'USO DELLA POSTA ELETTRONICA AZIENDALE 264
ESEMPIO 5 - GESTIONE DELLA VIOLAZIONE DEI DATI (DATA BREACH) 268

ALLEGATI 273

ALLEGATO A - FINALITÀ DEL TRATTAMENTO 275
ALLEGATO B - SOGGETTI INTERESSATI 279
ALLEGATO C - CATEGORIE DI DATI OGGETTO DI TRATTAMENTO 282
ALLEGATO D - SCENARI DI RISCHIO - RISORSE ESTERNE 284
IT-GRUNDSCHUTZ CATALOGUES 284
ENISA - THREAT TAXONOMY 285

ALLEGATO E - MISURE DI SICUREZZA - RISORSE ESTERNE 286
ENISA - HANDBOOK ON SECURITY OF PERSONAL DATA PROCESSING 286
CYBERSECURITY FRAMEWORK NAZIONALE 287
IT-GRUNDSCHUTZ CATALOGUES 289
NIST SPECIAL PUBLICATION 800-53 (REV. 4) 290
ALLEGATO F - POLICY E PROCEDURE - RISORSE ESTERNE 292
AUSTRALIAN GOVERNMENT INFORMATION SECURITY MANUAL 292
SANS INSTITUTE 296
ALLEGATO G - ANALISI DEI RISCHI E DPIA- RISORSE ESTERNE 298
AEPD 298
CNIL 299
ALLEGATO H - ANALISI DEI RISCHI - LISTADO DE CUMPLIMIENTO NORMATIVO 300
ALLEGATO I - ANALISI DEI RISCHI - RISORSE ESTERNE 302
ALLEGATO J - TRADUZIONE DELLE TABELLE ENISA 303
TABELLA 1 303
TABELLA 2 305
TABELLA 3 307
ALLEGATO K - ANALISI DEI RISCHI QUALITATIVA E QUANTITATIVA 308
UN CONFRONTO TRA I DUE APPROCCI 308
LA RACCOLTA DEI DATI 309
LE FONTI DI INFORMAZIONI 310
L'ATTRIBUZIONE DEI VALORI 311
SCALE QUALITATIVE 311
SCALE QUANTITATIVE 312
IL PROBLEMA DELLA RAPPRESENTAZIONE DEI VALORI STIMATI 312
CALCOLO DEL RISCHIO QUANTITATIVO 313
SOMMA O MOLTIPLICAZIONE? 315
CONCLUSIONI 317
ALLEGATO L - ASPETTI CONTRATTUALI NEI RAPPORTI CON OUTSOURCER/FORNITORI 318
OGGETTO 319
GESTIONE DEL CONTRATTO 319
MODALITÀ 320
RISPETTO DELLE NORME 321
RESPONSABILITÀ 323
CORRISPETTIVI 323
QUALITÀ DEL SERVIZIO 324
LA DESIGNAZIONE DEL SOGGETTO ESTERNO QUALE RESPONSABILE DEL TRATTAMENTO 325
ALLEGATO M - RISORSE ESTERNE 326
ALLEGATO N - GLOSSARIO 329

PRESENTAZIONE DELLA SECONDA EDIZIONE

PRESENTAZIONE DI GABRIELE FAGGIOLI

Tutti oggi leggono e parlano di sicurezza informatica.

Il tema è caldissimo e di grande interesse anche perché i casi che interessano le cronache sono, anche, impressionanti per mole di dati coinvolti e per l'importanza delle aziende colpite.

Non dobbiamo però mai dimenticare che la sicurezza informatica fa parte della vita di tutti noi, dei professionisti, degli artigiani, delle PMI, dei cittadini. Insomma, non bisogna necessariamente essere una azienda enterprise con miliardi di euro di fatturato per interessarsi del tema.

Inoltre, molti consulenti e DPO che offrono consulenza alle aziende e alle pubbliche amministrazioni spesso hanno estrazione legale e poca conoscenza delle tematiche di sicurezza.

Nel rispetto e ferma l'importanza delle competenze specialistiche è però ben possibile e direi necessario per tutti, professionisti, consulenti, DPO, privacy specialist, legali, ingegneri gestionali o economisti coinvolti in progetti tecnologici, iniziare ad avere una prima conoscenza del tema della sicurezza informatica soprattutto in un mondo altamente interconnesso come quello odierno.

Ecco allora che il libro di Giancarlo Butti, che ringrazio per la sempre importante collaborazione con il CLUSIT, viene incontro proprio a questa esigenza: formazione e cultura per tutti e, soprattutto, formazione multi-disciplinare.

Ci sarà chi si troverà più a proprio agio nel capitolo inerente la normativa applicabile, chi magari ha già conoscenza delle misure di sicurezza logiche o della gestione del rischio.

Il libro ha il grande pregio di proporre, per i non specialisti, una visione a 360 gradi.

Buona lettura!

Gabriele Faggioli
Presidente CLUSIT (Associazione Italiana per la Sicurezza Informatica)
www.clusit.it

PRESENTAZIONE DELLA PRIMA EDIZIONE

PRESENTAZIONE DI PAOLO GIUDICE

Giancarlo Butti, che ho conosciuto in quanto socio Clusit da diversi anni, si è sempre dimostrato molto attento e sensibile alle problematiche legate alla sicurezza delle informazioni e dal 2003 ad oggi ha realizzato numerose pubblicazioni su questi temi.

Con questo volume, che ha come tema la protezione dei beni aziendali, intesi come beni fisici, informazioni e persone, l'autore intende promuovere presso imprenditori e professionisti una giusta percezione dei rischi, proponendo un auto assessment e dando alcuni semplici consigli per elevare da subito il livello della sicurezza.

Non posso che essere riconoscente a Giancarlo per questo sforzo di divulgazione di una corretta cultura della sicurezza delle informazioni, che rientra tra le attività promosse e portate avanti dal Clusit.

Paolo Giudice
Segretario Generale CLUSIT (Associazione Italiana per la Sicurezza Informatica)
www.clusit.it

RECENSIONE DI SILVANO ONGETTA

Finalmente un testo che tratta di sicurezza informatica con un taglio differente dal consueto e che si rivolge non ai soliti addetti, ma a coloro che non sono del mestiere e hanno solo un'infarinatura di queste problematiche e devono per loro ventura identificare i beni materiali e immateriali da proteggere, individuare pragmaticamente le minacce che possono colpire quei beni, provvedere ad adeguate protezioni affinché le stesse rimangano lontane il più possibile dalla loro struttura e, giacché le risorse sono un'entità non infinita, gestire quantomeno il rischio residuo.

Semplice forse dirlo ma assolutamente non banale da realizzare se non si ha a fianco una guida che possa essere un buon compagno di banco.

Il libro ha a mio avviso la grande capacità di aprire un'ampia finestra anche sulle norme di comportamento che devono rappresentare il vademecum delle persone che con l'informatica e la sicurezza, devono convivere, sia in veste di addetti operativi del settore o che di utilizzatori finali.

Ho trovato molto apprezzabili i casi di studio riportati che offrono una visione grandangolare su alcuni esempi positivi di realtà aziendali di medio-piccole dimensioni in cui la sicurezza ha ricevuto un'accettabile attenzione. Casi emblematici in quanto in quel tipo di aziende di norma difficilmente opera un addetto con adeguate conoscenze/sensibilità della materia, ma soprattutto molto spesso l'imprenditore/titolare è poco incline a investire in sicurezza informatica se non costretto dalle norme di legge (ricordiamo che alcune hanno anche risvolti penali), per cui sovente confida nel sostanziale supporto del santo patrono locale. Il messaggio che ne diviene è che

anche in situazioni in cui sovente non si fa nulla per la sicurezza è possibile invece fare passi sostanziali affidandosi a un corretto approccio.

L'ultimo capitolo del libro riguarda le norme di legge sulla sicurezza, che in Italia in anni recenti ha ricevuto grande attenzione da parte delle Istituzioni Aver estratto gli articoli maggiormente pertinenti l'ho trovato meritorio soprattutto per l'approccio didattico volto ad avvicinare al dettame anche le persone che normalmente sono restie ad avventurarsi nel mondo leguleio.

Chiude il tutto un pregevole allegato di schede operative per inventariare i beni, i documenti, le misure adottabili…

Un particolare che mi piace sottolineare è che tranne alcuni termini ormai di uso corrente e un solitario DMZ, brilla l'assenza del puro informatichese e anche dell'inglese tipo-prezzemolo, così gradito a tanti autori in quasi spregio dei bellissimi equivalenti nella nostra lingua.

Una considerazione finale su alcuni spunti che oserei definire piccole perle – Giancarlo insiste tra le altre sulla necessità della formazione a tutti i livelli e sulle verifiche periodiche – due dei più importanti segreti per ottenere e mantenere un buon livello di sicurezza.

Silvano Ongetta
Presidente AIEA (Associazione Italiana Information Systems Auditors)
www.aiea.it

INTRODUZIONE

Questo libro si rivolge a chi non abbia una specifica competenza nell'ambito della sicurezza ed è chiamato, a vario titolo, a tutelare:

- i dati personali e i diritti e le libertà delle persone fisiche (in quanto Titolare, DPO, Responsabile…), secondo quanto previsto dalla normativa privacy[1]
- i beni della propria organizzazione, (gli asset aziendali, in quanto imprenditore, professionista, dirigente della PA…)
- il know how[2] aziendale.

Il libro è anche utile a quanti sono demandati a fornire supporto a tali soggetti nella valutazione del rischio e nella scelta e implementazione delle misure di sicurezza più idonee, permettendo di condividere un linguaggio comune il più possibile privo di una terminologia gergale.

Sono descritti, con linguaggio semplice, semplificato, discorsivo e, per quanto possibile, privo di termini tecnici, tutti i principali aspetti relativi alla sicurezza ed alla protezione dei beni materiali ed immateriali, compresi i dati personali, che costituiscono il patrimonio di un'organizzazione.

Un approccio didattico, che può agevolare nel loro lavoro anche i professionisti della sicurezza, che trovano in questo testo uno strumento per presentare argomenti non sempre facili da spiegare.

La prospettiva del libro è quella di dare indicazioni sulla gestione di rischi aziendali e delle relative contromisure nell'ottica di una visione sinergica, tesa a proteggere:

- gli asset aziendali
- i dati personali
- i diritti e le libertà delle persone fisiche
- il know how aziendale

al fine di tutelare l'azienda rispetto a:

- perdite:
    - economiche
    - di immagine
    - di clientela
    - di know how
- contenziosi legali
- sanzioni

[1] La normativa utilizza il termine protezione dei dati personali

[2] Il termine verrà meglio chiarito nei paragrafi successivi

- economiche
- penali
- blocco dei trattamenti.

I CONTENUTI DEL LIBRO

Il libro è composto da due parti.

Prima parte

La **prima parte** comprende una serie di capitoli descrittivi e didattici che descrivono il processo di valutazione del rischio sia dal punto di vista dei beni aziendali, sia dal punto di vista della normativa privacy (tutela dei diritti e delle libertà fondamentali delle persone fisiche).

Non trattandosi di un libro tecnico la modalità di presentazione delle informazioni vuole essere semplice e schematica, quasi una sorta di presentazione, una sequenza di slide e di tabelle che in breve esprimono i concetti più importanti.

Sta poi alla volontà del lettore approfondire le nozioni presentate nella parte descrittiva del testo; ulteriori approfondimenti sono possibili consultando la documentazione disponibile:

- nella seconda parte del libro e nelle appendici
- gratuitamente sui siti selezionati alla fine del testo.

La prima parte del libro è costituita da alcuni capitoli, corrispondenti ad altrettante fasi di un'analisi dei rischi.

Nel capitolo "***Gli asset da proteggere***" l'attenzione è focalizzata sulla identificazione degli asset aziendali, sulla loro valorizzazione, sulle loro interazioni. L'identificazione dei beni materiali da proteggere è relativamente semplice. Per quanto riguarda le informazioni (beni immateriali), l'indagine consente di individuare dove queste siano presenti all'interno dell'azienda: documenti, sistema informativo, prassi aziendale, conoscenze e competenze dei collaboratori, prototipi...; le informazioni sono quindi all'interno di asset materiali o costituiscono conoscenze e competenze di qualcuno.

Fra le informazioni sono ricompresi i dati personali, oggetto di particolare tutela in quanto presidiato da una corposa normativa, la cui violazione potrebbe avere conseguenza sui diritti e le libertà fondamentali delle persone fisiche (il vero oggetto di tutela della normativa privacy).

identificazione degli asset da proteggere (singolarmente o per classi omogenee) e delle relazioni esistenti fra asset diversi

identificazione dei dati trattati

identificazione dei soggetti interessati

identificazione delle finalità di trattamenti

identificazione delle minacce e delle vulnerabilità

valutazione delle probabilità

identificazione degli impatti diretti, indiretti, consequenziali e loro valorizzazione

valorizzazione del rischio

identificazione delle opportune misure di sicurezza in rapporto al costo/beneficio

gestione del rischio residuo

Nel capitolo ***"La gestione del rischio"*** si passa ad analizzare quelli che sono rischi, minacce, vulnerabilità…

Un bene materiale può essere rubato, danneggiato, distrutto; anche un'informazione può essere sottratta o cancellata, ma può anche essere copiata o intercettata senza alterare l'originale e quindi, senza che il proprietario se ne accorga.

Le minacce che incombono sulle informazioni sono quindi più estese e numerose di quelli dei beni materiali che le contengono.

La distruzione di un server ha un impatto sia per il valore intrinseco del bene, sia per quello dei dati in esso contenuti. Se quel server eroga un servizio importante per l'azienda (o per i suoi clienti), potrebbero esserci ulteriori conseguenze, quali l'interruzione del servizio, con ripercussioni di tipo economico, legale e di immagine.

Se i dati compromessi comprendessero anche dati personali, potrebbero esserci inoltre conseguenze sui diritti e le libertà delle persone fisiche.

L'analisi dei rischi connessa ad esempio alla perdita di un bene non si può limitare alla semplice valorizzazione monetaria dell'asset, ma deve valorizzare anche il reale impatto sul business aziendale, nonché sui diritti e le libertà delle persone fisiche.

Questa valorizzazione è indispensabile per permettere una corretta valutazione dei costi e benefici delle possibili contromisure, tenendo presente che i rischi sui diritti e le libertà delle persone fisiche, non sono rischi aziendali (e quindi nella disponibilità dell'azienda) e che quindi la loro gestione ha implicazioni specifiche.

Ad esempio, nel caso di rischio elevato la normativa prevede una specifica serie di adempienti, quali l'esecuzione di una DPIA.

Nel capitolo ***"Le misure di sicurezza"*** sono presentate numerose contromisure di natura organizzativa, fisica e logica ed i relativi processi di gestione.

È inoltre presente una raccolta di "***Norme di comportamento",*** che possono essere distribuite ai propri collaboratori.

Non si entra tuttavia nel dettaglio tecnico delle soluzioni, in quanto tale attività presuppone competenze specifiche.

Per l'implementazione delle contromisure tecniche è necessario rivolgersi a specialisti, mentre da subito è possibile mettere in atto contromisure di tipo organizzativo e comportamenti che possono ridurre notevolmente i rischi.

Ad esempio, per un commercialista la semplicissima regola di conservare presso il proprio studio solo le fotocopie dei documenti utili alla compilazione della dichiarazione dei redditi dei propri clienti, limita notevolmente il rischio legato alla loro distruzione o perdita (e le relative conseguenze legali, di immagine, ed economiche).

Il capitolo ***"Le normative sulla sicurezza"*** illustra le numerose normative che interessano la sicurezza in azienda: il GDPR, il D.lgs. 196/03, i numerosi Provvedimenti del Garante per la protezione dei dati personali, la normativa sui crimini informatici, quella sulla responsabilità amministrativa delle aziende, quella sulla firma digitale…

Parte seconda e appendici: strumenti operativi

Nella seconda parte del libro sono raccolte una serie di schede operative utili per il censimento degli asset aziendali e per la valorizzazione del rischio. In questo modo il lettore può fare immediatamente una prima analisi della propria situazione, valutando la propria esposizione al rischio e individuando le opportune contromisure.

Questo libro è pensato per chi, pur non avendo specifiche competenze nell'ambito della sicurezza, è chiamato a vario titolo a tutelare i dati personali e i diritti e le libertà delle persone fisiche (Titolari, DPO…) o gli asset aziendali tangibili o intangibili quali il know how (imprenditori, dirigenti…). Per i DPO costituisce un naturale complemento, per quanto riguarda gli aspetti di sicurezza, al manuale per i DPO pubblicato dall'Autorità Garante: The DPO Handbook.
Rispetto alla prima edizione il perimetro si è allargato per comprendere specificamente gli adempimenti previsti dal GDPR evidenziando, ad esempio, le differenze fra la valutazione dei rischi che incombono sugli asset aziendali rispetto a quelli che riguardano i diritti e le libertà delle persone fisiche.
Sono stati introdotti alcuni scenari che sempre più frequentemente interessano le organizzazioni, quali IOT, DLT, cloud, big data… elencandone i rischi per la privacy e la sicurezza e alcune possibili soluzioni.
La parte dedicata agli strumenti operativi è stata arricchita e sono stati inseriti numerosi allegati che rinviano anche a risorse esterne accessibili gratuitamente, mentre è stata sintetizzata la parte dedicata ai casi aziendali. La modulistica e le policy riportate nel volume sono disponibili on line.

DALLA PRESENTAZIONE ALLA SECONDA EDIZIONE
Tutti oggi leggono e parlano di sicurezza informatica...
Nel rispetto e ferma l'importanza delle competenze specialistiche è però ben possibile e direi necessario per tutti, professionisti, consulenti, DPO, privacy specialist, legali, ingegneri gestionali o economisti coinvolti in progetti tecnologici, iniziare ad avere una prima conoscenza del tema della sicurezza informatica soprattutto in un mondo altamente interconnesso come quello odierno.
Ecco allora che il libro di Giancarlo Butti, che ringrazio per la sempre importante collaborazione con il CLUSIT, viene incontro proprio a questa esigenza: formazione e cultura per tutti e, soprattutto, formazione multi-disciplinare...
Il libro ha il grande pregio di proporre, per i non specialisti, una visione a 360 gradi.

Gabriele Faggioli - Presidente CLUSIT (Associazione Italiana per la Sicurezza Informatica)

DALLA RECENSIONE ALLA PRIMA EDIZIONE
Finalmente un testo che tratta di sicurezza informatica con un taglio differente dal consueto e che si rivolge non ai soliti addetti, ma a coloro che non sono del mestiere e hanno solo un'infarinatura di queste problematiche e devono per loro ventura identificare i beni materiali e immateriali da proteggere, individuare pragmaticamente le minacce che possono colpire quei beni, provvedere ad adeguate protezioni affinché le stesse rimangano lontane il più possibile dalla loro struttura e, giacché le risorse sono un'entità non infinita, gestire quantomeno il rischio residuo.
Semplice forse dirlo ma assolutamente non banale da realizzare se non si ha a fianco una guida che possa essere un buon compagno di banco.
Il libro ha a mio avviso la grande capacità di aprire un'ampia finestra anche sulle norme di comportamento che devono rappresentare il vademecum delle persone che con l'informatica e la sicurezza, devono convivere, sia in veste di addetti operativi del settore o che di utilizzatori finali...
L'ultimo capitolo del libro riguarda le norme di legge sulla sicurezza, che in Italia in anni recenti ha ricevuto grande attenzione da parte delle Istituzioni. Aver estratto gli articoli maggiormente pertinenti l'ho trovato meritorio soprattutto per l'approccio didattico volto ad avvicinare al dettame anche le persone che normalmente sono restie ad avventurarsi nel mondo leguleio.
Chiude il tutto un pregevole allegato di schede operative per inventariare i beni, i documenti, le misure adottabili…
Un particolare che mi piace sottolineare è che tranne alcuni termini ormai di uso corrente e un solitario DMZ, brilla l'assenza del puro informatichese e anche dell'inglese tipo-prezzemolo, così gradito a tanti autori in quasi spregio dei bellissimi equivalenti nella nostra lingua.
Una considerazione finale su alcuni spunti che oserei definire piccole perle – Giancarlo insiste tra le altre sulla necessità della formazione a tutti i livelli e sulle verifiche periodiche – due dei più importanti segreti per ottenere e mantenere un buon livello di sicurezza.

Silvano Ongetta Past Presidente AIEA (Associazione Italiana Information Systems Auditors)

ISBN: 9788894441529

Prezzo € 34,00