Information & Cyber Security Strategy: cosa fare

Alessio L.R. Pennasilico

apennasi@clusit.it

Alessio L.R. Pennasilico aka -=mayhem=-

Practice Leader Information & Cyber Security Advisory Team @ P4I
Security Evangelist & Ethical Hacker

Membro del Comitato Tecnico Scientifico Clusit

Presidente dell'Associazione Informatici Professionisti AIP ITCS

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità Lloyd's Register LRQA

Membro del Comitato di schema kiwa intertek Total Quality. Assured.

Direttore Scientifico della testata CYBERSECURITY360

Perché è necessaria una Governance dei fornitori?

Molti incidenti si sono verificati a causa di una non corretta gestione di accessi o informazioni da parte dei fornitori

Le PMI potrebbero non avere le competenze per giudicare / verificare l'operato di tutti i propri fornitori

Le aziende di fascia enterprise, molto spesso, hanno come fornitori aziende non enterprise, quindi con maturità sui temi cyber e staff/capacità di investimento inferiori dei propri

Esempi

Forbes Billionaires Innovation Leadership Money Consumer Industry

64,334 views | Jan 10, 2014, 08:56am

Target Data Breach Spilled Info On As Many As 70 Million Customers

Maggie McGrath Forbes Staff

The data breach that was the nightmare before Christmas for Target TGT -1.3% and its millions of customers just got a little bit worse: the retailer said Friday morning that the information stolen between November 27 and December 15, 2013 included personal information of as many as 70

UniCredit

HOME > Press & Media > Comunicati stampa - Price sensitive > 2017 > Comunicato Stampa

SHARE PRINT SEND

Comunicato Stampa

26 luglio 2017 - h 08:56 | PRICE SENSITIVE Finanziario

UniCredit comunica di aver subito una intrusione informatica in Italia con accesso non autorizzato a dati di clienti italiani relativi solo a prestiti personali. Tale accesso è avvenuto attraverso un partner commerciale esterno italiano.

Secondo le risultanze della banca, una prima violazione sembra essere avvenuta nei mesi di settembre e ottobre 2016, mentre è stata appena individuata una seconda intrusione avvenuta nei mesi di giugno e luglio 2017. Si ritiene che nei due periodi siano stati violati i dati di circa 400.000 clienti in Italia. La banca precisa che non è stato acquisito nessun dato, quali le password, che possa consentire l'accesso ai conti dei clienti o che permetta transazioni non autorizzate. Potrebbe invece essere avvenuto l'accesso ad alcuni dati anagrafici e ai codici IBAN.

UniCredit ha informato le autorità competenti ed ha avviato uno specifico audit sul tema. In mattinata, formalizzerà altresì un esposto presso la Procura della Repubblica di Milano. La banca ha inoltre immediatamente adottato tutte le azioni necessarie volte ad impedire il ripetersi di tale intrusione informatica.

UniCredit mette a disposizione il numero verde dedicato 800 323285 per i clienti che desiderino ulteriori informazioni. Il personale della propria filiale di riferimento è naturalmente a disposizione per qualsiasi ulteriore informazione. La banca contatterà i clienti interessati mediante canali di comunicazione specifici. Per ragioni di sicurezza non verranno utilizzate la posta elettronica o le telefonate dirette.

La tutela e la sicurezza dei dati dei propri clienti sono per UniCredit una assoluta priorità e nell'ambito del recente piano industriale Transform 2019 il gruppo sta investendo 2,3 miliardi di euro per rafforzare e rendere sempre più efficaci i propri sistemi informatici.

Milano, 26 luglio 2017

PCWorld FROM IDG

File-Sharing Site MegaUpload Indicted for Internet Piracy, Shut Down by US

By Megan Geuss and David Daw, PCWorld
Jan 19, 2012 3:25 PM

MEGAUPLOAD

MegaUpload.com, one of the Internet's best-known file-sharing sites, was shuttered by federal officials Thursday. In addition, founder Kim Dotcom (formerly Kim Schmitz) and three other executives connected to the parent company MegaUpload Limited were arrested in New Zealand.

Ma quali fornitori?

Una corretta strategia di tutela delle informazioni
oltre a prendere in considerazione solo i fornitori ICT
considera tutti i fornitori che accedono o gestiscono informazioni aziendali

NB: per alcune tipologie di informazioni esistono obblighi di compliance, si pensi al GDPR relativamente ai dati personali o alle normative specifiche per banche, assicurazioni, telco, etc.

Cosa fare?

Conoscere i propri asset
Determinare i requisiti
Contrattualizzare i requisiti
Verificare che il contratto venga rispettato

Conoscere i propri asset

Per poter assegnare in modo sostenibile
i criteri di protezione alle informazioni
è opportuno **creare alcune categorie predefinite di informazioni**

Si rende poi necessario conoscere
quali informazioni l'Organizzazione possiede
ed a **quale categoria** appartengano

Esempio

Creare una propria politica di classificazione delle informazioni, requisito tra gli altri della ISO/IEC 27001:2013, permette di creare dei cluster di informazioni rispetto al livello di riservatezza. Dalla Business Impact Analysis aziendale, invece, è possibile ricavare il livello di disponibilità necessario.
La tabella sotto semplifica la matrice che si potrà creare:

Cluster	Riservatezza	Necessità di Disponibilità
0-1-2	Pubbliche	Bassa - Media - Alta
3-4-5	Riservate	Bassa - Media - Alta
6-7-8	Confidenziali	Bassa - Media - Alta
9-10-11	Strettamente confidenziali	Bassa - Media - Alta

Esempio semplificato

Esempio

Creati i cluster di informazioni è necessario catalogare le informazioni presenti in azienda ed assegnarle alle diverse categorie

Dove trovo elenchi di informazioni aziendali?

Es. Per chi ha intrapreso un progetto di data governance nel data catalog
Es. Per chi ha fatto un registro dei trattamenti ex art. 30 GDPR nel registro

Per chi non ha informazioni pregresse le tecniche di data discovery proprie della data governance, e degli strumenti afferenti, possono essere di aiuto

Determinare i requisiti

Andrà quindi creato un modello di controlli
associato ad ogni cluster di informazioni gestite

I controlli potranno essere anche tecnici,
ma non vanno dimenticati quelli organizzativi, legali, etc.

Questo permetterà di creare dei cluster di fornitori, abilitati a lavorare su alcuni cluster di informazioni

Esempio

E’ possibile selezionare i controlli tecnologici
da diverse best practice e standard

ISO 20000-1:2011
(Delivery of IT service)

ISO 22301:2012
(Business Continuity)

ISO:IEC 27000 series
(Information Security Management)

NIST Cyber Security Framework

ANSI/ISA 62443
(Security for industrial automation and control systems)

PCI-DSS 3.2
(Electronic payments)

CSA STAR
(Cloud Security Alliance)

Technical Assessment (e.g. Critical Security Controls, OWASP Testing Guide, NIST 800-53A, etc.)

Esempio

E’ possibile ad esempio richiedere per l’accesso ad alcuni cluster di informazioni una certificazione specifica (es. ISO/IEC 27001:2013) o il rispetto di un set di controlli equivalenti

La certificazione, evidentemente, semplifica il processo di risposta del fornitore e semplifica la verifica da parte del Cliente

Da non trascurare, per i fornitori ICT, le certificazioni vendor based, per chi propone le specifiche tecnologie

Esempio

E’ possibile selezionare i controlli non tecnologici secondo una propria policy che può tener conto di molti altri aspetti non tecnologici.

Esempi:

- *Presenza di un CIO, di un CISO, di un DPO, etc etc*
- *Numero di collaboratori, fatturato, rilevanza del Cliente sul fatturato*
- *Numero di sedi*
- *Referenze*
- *Etc.*

Esempio

Come determinare la presenza di alcuni requisiti?

Esempio:

1. *Analisi del procurement (es. visura camerale)*
2. *Questionario in self assessment*
3. *Audit*
4. *Dichiarazioni allegate allegate al contratto*
5. *Etc.*

Contrattualizzare i requisiti

I requisiti vanno poi riportati nei contratti

Diventa essenziale quindi stabilire, ad esempio:
SLA, KPI, modalità di monitoraggio, frequenza di monitoraggio, modalità di monitoraggio, etc.

I quali influenzeranno, ad esempio:
penali, clausola risolutiva espressa, etc.

Esempio

Nell'affidamento della gestione di una applicazione web si potrebbe ipotizzare un criterio oggettivo di misurazione che influenzi le attività:

Esempio:

- *In fase di consegna del progetto verrà eseguito un Penetration Test Applicativo da una società terza, **prima di andare in produzione***
- *Ogni vulnerabilità appartenente alla OWASP Top 10 verrà considerata vizio di fabbricazione e precluderà il collaudo fino alla sua risoluzione*
- *Lo stesso processo verrà eseguito durante la manutenzione, per ogni major release*
- *Per ogni minor release verrà eseguito un vulnerability scan dal Cliente*
- *In quanto vizio di fabbricazione il fornitore nulla potrà addebitare per la risoluzione di tali vulnerabilità*
- *Tali vulnerabilità dovranno essere risolte in massimo X gg lavorativi*
- *Ogni ulteriore giorno necessario alla risoluzione comporterà una penale di € Y*
- *La mancata risoluzione nei tempi concordati di tali vulnerabilità nei tempi stabiliti per più di Z volte comporterà la facoltà da parte del Cliente di avvalersi della clausola di risoluzione espressa*
- *Etc.*

Verificare che il contratto venga rispettato

Se selezionare il fornitore adatto è un tema strategico,
è imprescindibile la necessità di verificare
che i controlli concordati siano applicati uniformemente nel tempo

Per questa ragione è indispensabile stabilire ed eseguire un piano di audit
secondo le modalità concordate contrattualmente

Esempio:
verifiche da remoto, verifiche in loco, verifiche da parti terze, etc.

Monitoraggio dei fornitori

Un approccio simile a quello presentato permetterà nel tempo di

creare delle statistiche sull'efficacia della selezione dei fornitori
comprendere quanti e quali cluster creano maggiori anomalie
rivedere i criteri di selezione e monitoraggio per affinarli

Ma chi si deve occupare di questi temi?

Un framework di gestione dei fornitori richiede che diverse funzioni aziendali, con diverse competenze collaborino attivamente e costantemente per la corretta applicazione del framework stesso

Sono necessarie le funzioni, ad esempio:

- *Procurement*
- *Legal Affair*
- *Compliance*
- *ICT*
- *Security*

Solo per citarne alcune!

Conclusioni

Il rischio di fornitura è uno dei pillar
dell'Enterprise Risk Management (ERM)

Il Cyber Risk legato ai fornitori deve essere uno degli aspetti valutati e gestiti
non solo per i fornitori ICT

Il legame con i Compliance Risk è sempre più forte

Conclusioni

Per tutte queste ragioni diventa indispensabile dotarsi di
un framework integrato per la gestione dei fornitori
che prenda in considerazione tutti i necessari aspetti

Tale framework dovrà quindi tener conto di
esigenze di tutela del business, esigenze di rispetto della compliance
richiedendo quindi un approccio di competenze integrate

GRAZIE!

Alessio Pennasilico

Comitato Tecnico Scientifico
apennasi@clusit.it