GDPR

Il nuovo Regolamento Privacy Europeo

Sicurezza Informatica

Prevenzione, protezione dei sistemi, obblighi e responsabilità dei Titolari

Ing. Giorgio Montù

CONSULENTI
PRIVACY TORINO

2017 – Allarme rosso

1° semestre del 2017 : il peggiore di sempre nell'evoluzione delle minacce «cyber» e relativi impatti, sia dal punto di vista quantitativo che qualitativo.

Rapporto Clusit (Associazione Italiana per la Sicurezza Informatica) 2017 sulla sicurezza ICT in Italia

CONSULENTI
PRIVACY TORINO

Alcuni dei principali attacchi a livello globale 2016 -2017

	Vittima	Attaccante	Tecniche usate
1	Hollywood Presbyterian Medical Center[17]	Cyber Crime	Ransomware

L'attacco basato su ransomware ha costretto l'ospedale, a fronte del blocco del sistema informativo e quindi delle attività cliniche, causato dalla cifratura dei propri dati (strutturati e non strutturati), a pagare un riscatto di 17.000 USD per ottenere dai criminali la chiave di decifratura.

	Vittima	Attaccante	Tecniche usate
3	Bangladesh Bank[19]	Cyber Crime	Multiple

Una delle più grandi cyber-rapina di tutti i tempi, e probabilmente la più grande del 2016, è stata compiuta ai danni della Banca del Bangladesh, con un danno stimato in 81 milioni di dollari.
Gli attaccanti, dopo aver compromesso alcuni sistemi della banca, hanno introdotto nel sistema SWIFT transazioni fraudolente ordinando il trasferimento di fondi per un totale di 1 miliardo di dollari, delle quali fortunatamente (per un banale errore da parte dei criminali) solo la prima tranche da 81 milioni è andata a buon fine.

CONSULENTI PRIVACY TORINO

Alcuni dei principali attacchi a livello globale 2016 -2017

4	Vittima	Attaccante	Tecniche usate
	ADUPS Technology[20]	Cyber Espionage (Cina?)	Multiple

I sistemi della società cinese ADUPS Technology sono stati violati, consentendo agli attaccanti di modificare il firmware per device Android prodotto dall'azienda, installato su 700 milioni di macchine commercializzate da numerosi vendor in diversi paesi del mondo, introducendovi una backdoor.
Il firmware così infettato raccoglieva informazioni relative a IMEI, IMSI, MAC address, version number, operatore telefonico, SMS ed elenco delle chiamate, ed ogni 72 ore le inviava in background ad un server remoto in Cina. L'attività di data collection è durata oltre 6 mesi prima di essere scoperta

6	Vittima	Attaccante	Tecniche usate
	Democratic National Committee (DNC)[22]	Cyber Espionage (Russia?)	Multiple

Wikileaks ha pubblicato 19.252 email relative al Comitato Nazionale del Partito Democratico, ai suoi vertici ed ai suoi collaboratori, alcune delle quali piuttosto compromettenti, in quanto sembrerebbero indicare che il partito abbia favorito la candidatura di Hillary Clinton sfavorendo il candidato Bernie Sanders.
Le email sono state sottratte (ufficialmente) da un hacker dal nickname Guccifer 2.0, anche se tutte le principali agenzie di intelligence americane hanno dichiarato di avere prove dell'intervento russo dietro le quinte della vicenda.
La questione ha creato scandalo ed occupato i media per mesi, e probabilmente influito in qualche misura sull'esito elettorale, prefigurando così scenari inediti di Psychological Operations (PsyOps), e dimostrando la possibilità di interferire pesantemente con mezzi "cyber" nella vita democratica delle nazioni.

CONSULENTI
PRIVACY TORINO

Alcuni dei principali attacchi a livello globale 2016 -2017

Attacchi a qualcuno che conosciamo bene

7	Vittima	Attaccante	Tecniche usate
	Yahoo[23]	Cyber Crime	Multiple

Il data breach più importante della storia (oltre un miliardo di account sarebbero stati violati) è avvenuto ai danni di Yahoo e dei suoi utenti. Gli attaccanti avrebbero sottratto nomi, indirizzi email, numeri di telefono, date di nascita, password criptate e in qualche caso anche domande di sicurezza cifrate o in chiaro, con le relative risposte, che poi sarebbero stati messi in vendita in alcuni marketplace del dark web, per circa 300.000 USD.
Anche a causa di questo data breach (e di altri data breach precedenti, non comunicati tempestivamente dall'azienda), alcuni analisti finanziari sostengono che la quotazione di Yahoo nell'ambito dell'acquisizione in corso da parte di Verizon sia stata ribassata di circa 350 milioni di USD[24].

CONSULENTI
PRIVACY TORINO

Alcuni dei principali attacchi a livello globale 2016 -2017

I cyber criminali si sono avvalsi di un nome riconosciuto come quello di Vodafone per spingere gli utenti ad aprire un link che, tramite un exploit per Microsoft Explorer, permetteva il download e l'esecuzione di programmi arbitrari dal web. Anche in questo caso l'attacco è stato utilizzato per la diffusione del ransomware CryptoLocker. In altri casi simili sono stati utilizzati altri marchi conosciuti per l'invio di email di spam apparentemente lecite. Tra le campagne principali quelle che fanno riferimento a "*Cartella esattoriale Equitalia*", "*Pacco DHL in consegna*", "*Fattura Telecom»*

CONSULENTI PRIVACY TORINO

Alcuni dei principali attacchi a livello globale 2016 -2017

CORRIERE DELLA SERA / POLITICA

FISCO E PRIVACY

Buco nel sistema: fatture elettroniche online. Indagano Garante e Vigilanza

Con un semplice codice fiscale si potevano vedere e scaricare le fatture telematiche trasmesse all'Agenzia delle Entrate. L'Ad Ruffini «nero», chiede una relazione alla Sogei. Il presidente della Vigilanza parlamentare «furibondo». Il Garante chiede lumi.

di Mario Sensini

C'era un buco enorme nel sistema telematico gestito dalla società pubblica Sogei per la trasmissione delle fatture elettroniche all'Agenzia delle Entrate. Una falla che ha permesso a chiunque avesse le credenziali per entrare, commercialisti o anche semplici contribuenti, e per non si sa quanto tempo, di consultare liberamente i dati fiscali degli altri cittadini.

CONSULENTI PRIVACY TORINO

MI-GM4

Alcuni dei principali attacchi a livello globale 2016 -2017

Più vicino a noi: UNICREDIT

DAVIDE LESSI
TORINO

PUBBLICATO IL 26/07/2017
ULTIMA MODIFICA IL 26/07/2017 ALLE ORE 19:46

Un doppio attacco informatico su larga scala. Che ha coinvolto in tutto 400 mila clienti italiani di UniCredit. La prima intrusione nel 2016, la seconda pochi giorni fa. È stato lo stesso istituto di credito a dare i dettagli dell'hackeraggio assicurando, però, che **non sono stati acquisiti dati per l'accesso ai conti o che permettano transazioni non autorizzate.** L'attacco sarebbe avvenuto attraverso un partner commerciale italiano esterno.

CONSULENTI
PRIVACY TORINO

MI-GM5

Alcuni dei principali attacchi a livello globale 2016 -2017

Ancora più vicino: MAN IN THE MAIL

Da **Striscia la Notizia:**

http://www.striscialanotizia.mediaset.it/video/man-in-the-email_23253.shtml

CONSULENTI
PRIVACY TORINO

MI-GM6

Alcuni dei principali attacchi a livello globale 2016 -2017

In mezzo a noi

In questa sala ……

CONSULENTI
PRIVACY TORINO

D.Lgs. 196/2003 – ancora in vigore

Allegato B – Disciplinare tecnico in materia di misure minime di sicurezza

- Gestione profili di autorizzazione e credenziali di autenticazione
- Sistema antivirus e antispam
- Aggiornamento periodico (almeno semestrale) dei sistemi
- Backup dei dati con cadenza almeno settimanale
- Istruzioni tecnico-organizzative per gestione e salvataggio datiò
- Definizione di procedure per garantire il ripristino dell' accesso ai dati
- DPSS (successivamente abrogato)
- Successivo provvedimento LOG Amministratori di sistema (12/2009)

CONSULENTI
PRIVACY TORINO

Misure minime di sicurezza

Cosa succede dal 25 maggio 2018?

Il Garante italiano deve ancora fornire linee guida relative all'applicazione delle misure di sicurezza ed eventualmente introdurre nuove misure minime di sicurezza, o mantenere le attuali…

Cambierà certamente la modalità di applicazione…

CONSULENTI
PRIVACY TORINO

ACCOUNTABILITY

- Il Regolamento stabilisce la **responsabilizzazione** (accountability) del Titolare del trattamento

- Il Titolare ha l'obbligo di **dimostrare** la compliance alle prescrizioni del Regolamento mediante l'adozione di **misure tecniche** (per la sicurezza fisica e informatica dei dati) **e organizzative** (politiche e procedure interne, formazione del personale, verifiche o audit…) adeguate, nonché un **apparato documentale** appropriato

- Adesione a **codici di condotta** o meccanismi di **certificazione**

CONSULENTI
PRIVACY TORINO

GDPR – Sicurezza del trattamento

Art. 5 – Principi applicabili al trattamento dei dati personali

1. I dati personali sono:

…

F) Trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante

misure tecniche e organizzative adeguate

da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)

CONSULENTI
PRIVACY TORINO

GDPR – Sicurezza del trattamento
Cosa fare

Analisi dei rischi

Deve tenere conto di:

- Eventualità di distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzati a dati personali trasmessi, conservati o elaborati

- Eventuali pregiudizi derivati: danni fisici, materiali o immateriali

- Elevatezza del rischio

Il rischio va valutato in base alla sussistenza, frequenza, gravità

CONSULENTI
PRIVACY TORINO

GDPR – Sicurezza del trattamento
Cosa fare

Contromisure tecniche adeguate

Effettivamente in grado di contrastare:
- distruzione
- perdita
- modifica
- divulgazione non autorizzata
- accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati

CONSULENTI
PRIVACY TORINO

GDPR – Sicurezza del trattamento

Art. 32 – Sicurezza del trattamento

Tenendo conto dello stato dell'arte, dei costi di attuazione, del contesto e delle finalità del trattamento, prevede:

- misure tecniche ed organizzative adeguate per garantire un **livello di sicurezza adeguato al rischio**
- **pseudonimizzazione e cifratura dei dati** (se del caso)
- assicurare **riservatezza**, **integrità**, **disponibilità** e **resilienza** dei sistemi
- capacità di **ripristinare** tempestivamente la **disponibilità e l'accesso dei dati**
- **procedura per verificare e valutare** regolarmente l'efficacia delle misure tecniche e organizzative

CONSULENTI
PRIVACY TORINO

GDPR – Sicurezza del trattamento
Cosa fare

Contromisure tecniche minime vs adeguate – qualche esempio

- per contrastare malware tipo Cryptolocker: Antivirus e antispam / email gateway o specifici firewall avanzati
- Sicurezza ripristino dei dati: backup settimanale su unico supporto / backup giornaliero + settimanale + mensile su più supporti, anche delocalizzati o in cloud
- Intrusioni indesiderate: firewall tradizionale / sistemi firewall con servizi avanzati e di «controllo» della navigazione

Altri esempi di misure adeguate: connessioni dall'esterno tramite VPN, utilizzo password complesse e cambio a intervalli più ravvicinati, disattivazione degli account non piu' utilizzati , affinamento delle misure tecniche ritenute adeguate in funzione dei tempi di ripristino auspicati (business continuity), etc. ….

CONSULENTI
PRIVACY TORINO

GDPR – Sicurezza del trattamento
Cosa fare

Contromisure organizzative adeguate (obbligatorie o consigliate dai legislatori)

- Formazione obbligatoria degli addetti al trattamento dei dati
- Regolamentazione dell' utilizzo sistemi informatici/telematici
- Adozione di procedure per la verifica dell'adeguatezza delle misure tecniche adottate
- Adesione a codici di condotta o certificazioni specifiche (p.e. ISO 27001)

CONSULENTI
PRIVACY TORINO

GDPR – Sicurezza del trattamento

Art. 33 – Data Breach

In caso di violazione dei dati personali **il Titolare notifica la violazione all'autorità Garante entro 72 ore e deve**

- Descrivere la **natura della violazione** dei dati personali, le categorie e il numero approssimativo di interessati, nonché le categorie e il numero approssimativo delle registrazioni
- Comunicare il **nome e i dati di contatto del responsabile della protezione dei dati** o altro punto di contatto
- Descrivere le probabili **conseguenze della violazione** dei dati personali
- Descrivere le **misure adottate** o di cui si propone l'adozione per **porre rimedio** alla violazione e, se del caso, **per attenuare** i possibili **effetti negativi**

CONSULENTI
PRIVACY TORINO

GDPR – Sicurezza del trattamento

Art. 34 – Data Breach

Quando la violazione presenta un **rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare comunica la violazione all'interessato** senza giustificato ritardo:

- Descrivendo con un linguaggio semplice e chiaro la **natura della violazione** dei dati personali
- Comunicando il **nome e dati di contatto del responsabile della protezione dei dati** o altro punto di contatto
- Descrivere le probabili **conseguenze della violazione** dei dati personali
- Descrivere le **misure adottate** o di cui si propone l'adozione per **porre rimedio** alla violazione e, se del caso, **per attenuare** i possibili **effetti negativi**

CONSULENTI
PRIVACY TORINO

GDPR – Sicurezza del trattamento

Art. 34 – Data Breach

Non è richiesta la comunicazione della violazione all'interessato se:

- Il Titolare ha messo in atto **misure tecniche ed organizzative adeguate** ed erano state applicate ai dati personali oggetto di violazione, in particolare la **cifratura**
- Il Titolare ha successivamente adottato misure per **scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati**
- La comunicazione richiedesse **sforzi sproporzionati,** in tal caso si procede tramite **comunicazione pubblica**

CONSULENTI
PRIVACY TORINO